2020

ESTABLISHMENT OF CYBER-PHYSICAL CORRELATION AND VERIFICATION BASED ON ATTACK SCENARIOS IN POWER SUBSTATIONS

Koji Yamashita
Michigan Technological University, kyamashi@mtu.edu

ESTABLISHMENT OF CYBER-PHYSICAL CORRELATION AND VERIFICATION BASED ON ATTACK SCENARIOS IN POWER SUBSTATIONS

By

Koji Yamashita

A DISSERTATION

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

In Electrical Engineering

MICHIGAN TECHNOLOGICAL UNIVERSITY

2020

This dissertation has been approved in partial fulfillment of the requirements for the Degree of DOCTOR OF PHILOSOPHY in Electrical Engineering.

Department of Electrical and Computer Engineering

Dissertation Advisor:	*Dr. Chee-Wooi Ten*
Committee Member:	*Dr. Yeonwoo Rho*
Committee Member:	*Dr. Kui Zhang*
Committee Member:	*Dr. Nanpeng Yu*
Department Chair:	*Dr. Glen E. Archer*

Contents

List of Figures

List of Tables

Acknowledgments

I would like to thank all those who have helped me learn, understand and appreciate this subject, including

† My advisor, Prof. Chee-Wooi Ten

† Prof. Cheng-Ching Liu

† Now-dead Prof. Yasuo Tamura

† Dr. Shinichi Iwamoto

† Dr. Toshio Inoue

† Prof. Lingfeng Wang

† Prof. Wei Wei

† Mr. Andrew Ginter

† Prof. Jin Ma

† Prof. Su Su

† Prof. Nanpeng Yu

† Mr. Hayato Satoh

.

List of Abbreviations

AVR	Automatic Voltage Regulator
AGC	Automatic Generator Control
CB	Circuit Breaker
CPU	Central Processing Unit
CIP	Critical Infrastructure Protection
CPPS	Cyber-Physical Power System
CPS	Cyber-Physical System
CRIEPI	Central Research Institute of Electric Power Industry
DDoS	Distributed Denial of Service
DOE	Department of Energy
DoS	Denial of Service
EMS	Energy Management System
ESS	Energy Storage System
FACTS	Flexible AC Transmission System
GSPN	Generalized Stochastic Petri-net
HIL	Hardware In the Loop
ICT	Information and Communications Technology
IDS	Intrusion Detection System

IEC	International Electric Commission
IED	Intelligent Electronic Device
IP	Internet Protocol
LFC	Load Frequency Control
NERC	North America Electric Reliability Corporation
OEL	Over Excitation Limiter
OS	Operating System
RTDS	Real-Time Digital Simulator
SCADA	Supervisory control And Data Acquisition
SIPS	System Integrity Protection System
SPS	Special Protection Scheme/System
SVC	Static Var Compensator
STATCOM	Static synchronous Compensator
WAMPAC	Wide-area Measurement, Protection and Control

Abstract

Insurance businesses for the cyberworld are an evolving opportunity. However, a quantitative model in today's security technologies may not be established. Besides, a generalized methodology to assess the systematic risks remains underdeveloped. There has been a technical challenge to capture intrusion risks of the cyber-physical system, including estimating the impact of the potential cascaded events initiated by the hacker's malicious actions.

This dissertation attempts to integrate both modeling aspects: 1) steady-state probabilities for the Internet protocol-based substation switching attack events based on hypothetical cyberattacks, 2) potential electricity losses. The phenomenon of sequential attacks can be characterized using a time-domain simulation that exhibits dynamic cascaded events. Such substation attack simulation studies can establish an actuarial framework for grid operation.

The novelty is three-fold. First, the development to extend features of steady-state probabilities is established based on 1) modified password models, 2) new models on digital relays with two-step authentications, and 3) honeypot models. A generalized stochastic Petri net is leveraged to formulate the detailed statuses and transitions of components embedded in a Cyber-net. Then, extensive modeling of steady-state

probabilities is qualitatively performed. Methodologies on how transition probabilities and rates are extracted from network components and actuarial applications are summarized and discussed.

Second, dynamic models requisite for switching attacks against multiple substations or digital relays deployed in substations are formulated. Imperative protection and control models to represent substation attacks are clarified with realistic model parameters. Specifically, wide-area protections, i.e., special protection systems (SPSs), are elaborated, asserting that event-driven SPSs may be skipped for this type of case study.

Third, the substation attack replay using a proven commercially available time-domain simulation tool is validated in IEEE system models to study attack combinations' critical paths. As the time-domain simulation requires a higher computational cost than power flow-based steady-state simulation, a balance of both methods is established without missing the critical dynamic behavior. The direct impact of substation attacks, i.e., electricity losses, is compared between steady-state and dynamic analyses. Steady-state analysis results are prone to be pessimistic for a smaller number of compromised substations.

Finally, simulation findings based on the risk-based metrics and technical implementation are extensively discussed with future work.

Chapter 1

Introduction

The year 2019 marked the tenth anniversary of enforcement for North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance [1]. The latest version of NERC CIP compliance represents an ongoing refinement in compliance derived from the first draft of CIP002-CIP009 in 2005 [2]. Security violations have been reported recently with fines [3]. Apparently, historical events of cyber anomalies that are occurred over the past 15 years [4] are rooted in the facts where many believe that these cyber-physical security issues in control centers and substations must be carefully planned for the imminent security threats. In general, there are two groups of asset owners, *i.e.*, ones would either aim to (1) ensure 100% compliance and move on with a minimum investment plan, or (2) comply with a high desire to know how to invest and better protect their cyber-infrastructure with

new security technologies. Although the current processes of compliance are thorough and evidence-based, it does not adequately address specific technologies that would enhance security measures to deter potential intrusions. This reflects systemic risk in numbers that can be used for audits [5].

The convenient remote access to Internet Protocol (IP)-based substations elevates security concerns [6, 7, 8]. It becomes a balancing decision between security and maintenance as there are no perfect technologies to thwart uninvited "guests" effectively [9]. NERC CIP strongly recommends deploying an analytic of anomaly detection features across all IP-based substations. Statistically, the anomalies are the electronic evidence that sometimes can be used for forensic investigation, although the downside would be being subject to tamper if attackers find out where the security logs are stored. This source of security logging can be very useful in establishing a security profile.

Direct security patches and updates are not permitted in a live control system. Hence, the prevention of a cyber attack can be challenging, particularly with the increasing number of unpatched software vulnerabilities that might not effectively reflect on an organization's security posture [10, 11]. One of the key countermeasures is risk management that consists of the associated portfolios and assessment as well as the emergency response. These residual risks require extraction within a cyber network where this information can be consolidated and processed to make a meaningful

conclusion for analysis of compliance. With digital protective relaying, the support of IEC61850 can maximize the performance and reliability of the control system [12, 13]. The new deployment of IP-based intelligent electronic devices (IEDs) can post a security threat to be manipulated by attackers [14, 15, 16, 17].

One security technology that may not be well integrated into critical infrastructure as part of the security solutions is the honeypots/honeynet framework. Such technology has been used to cope with the malware that is a source of spreading security threats [18, 19]. Generally, the honeynet is a fictitious network that consists of a virtual firewall and servers (honeypots) that can be rephrased as a fake network representation, *i.e.*, a decoy. The honeynet was not widely used as compared to the intrusion detection system (IDS); honeynet can be a steppingstone to facilitate unauthorized access and to spread worms. The malware becoming apparent that can be automated to increase the trial-and-error rate to discover network architecture details and entities within a network. This can be revealed through their unauthorized access and footprint. On the contrary, the current countermeasure may not be adopted in a more proactive manner to promote risk awareness, although honeynet can be a technology for deployment [20].

The overarching question here is that how the stakeholder community would conform to a systematic evaluation of the cyber system based on the discrete events of intrusion processes and modeling of hypothetical disruptive attacks at the substations. The

primary contribution of this work is to establish an actuarial framework to measure the systemic risk of the cyber system based on security technologies deployed in IP-based substations using four Petri net models: firewall, password, IED, and honeynet models. This work is connected with a discussion in the later section based on industry practice in security logging and how this can be beneficial to redefine grid security.

1.1 Systemic Risk Modeling and Contributions

Fig. 1.1 shows how systemic risk can be formulated based on countermeasure, technologies, and methods. This dissertation establishes a comprehensive elaboration of modified and updated cyber-net with new models of IEDs and the honeypot/honeynet connecting the modified password and firewall models, as shown in Fig. 1.2.

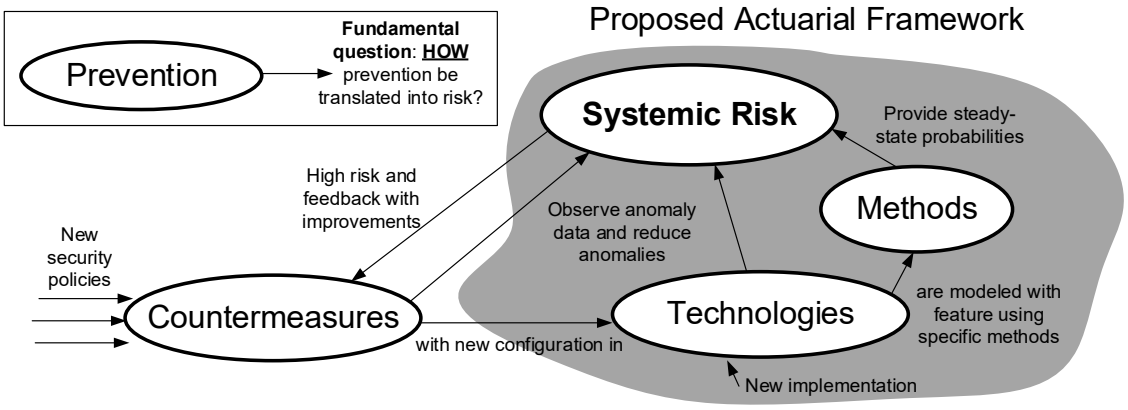


Figure 1.1: Systemic risk modeling and anomaly data synthesis [21]

The switching attack that opens circuit breakers at substations may be performed not only via local substation supervisory control and data acquisition (SCADA), but also through direct IED connections compromised that enables plotting for cyber-physical system (CPS) switching attacks (see pink arrows pointing to substations in Fig. 1.3).

It is noted that the CPS in the power grid consists of a cyber system and a physical system. The cyber system represents control and protection systems in the power system highlighted in orange (Fig. 1.3).

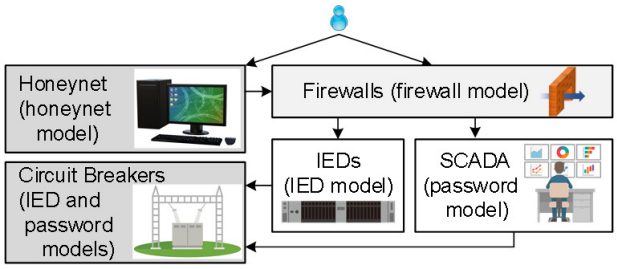


Figure 1.2: Interdependencies of abstracted models in a cyber-net [21]

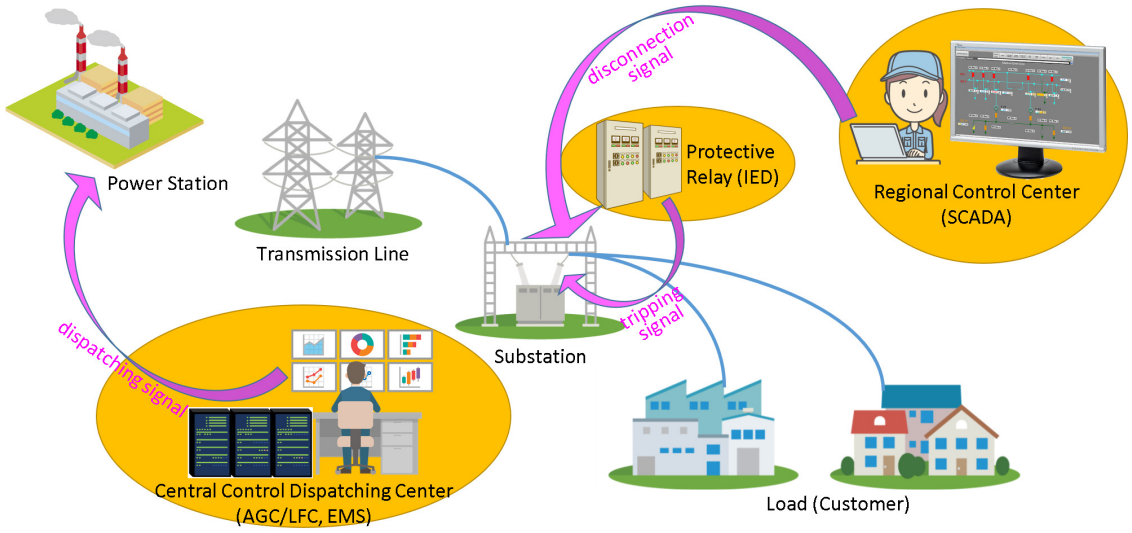


Figure 1.3: Systemic risk modeling and anomaly data synthesis

Hackers' targets are power equipment, and they often want to deenergize them or incur operational issues to cause power outages.Generally speaking, hackers need two steps to make this happen.The first step is to crack protection and control systems in the cyber system, highlighted by orange in Fig. 1.3.The second step is to send false commands or signals to the targeted system, illustrated in the pink arrows in Fig. 1.3. Therefore, the hacker attacks both the cyber system and the physical system. Such attacks are called *coordinated attacks*.

Capturing the intrusion processes and behaviors of attackers within the private networks with security technologies of defender should be characterized in formalism for the description of concurrency and synchronization for the computational problems [22, 23]. For decades, the Petri net is utilized as an *automaton* to model between finite-state and machines as well as to analyze the capabilities [24]. In a more recent development on the cyber-physical system for the power grid, a preliminary model establishment using the steady-state probability was introduced [25, 26].

The disruptive switching substation attack through the server is modeled; however, the switching attack through IEDs such as digital protective relays is not explicitly modeled. The latest security technology, such as new security policies, can be incorporated.

Other applications also gain attention in this subject and extend research in performance evaluation, such as the control system in the nuclear power station [27], the

energy control center [28], the impact analysis of the intrusion detection, and the response of cyber-physical systems [29]. References [27, 28, 29, 30] adopt a Petri net model mainly to derive the reliability and availability of the system for the cyberattack. Although emerging issues on cyber insurance are discussed in [30, 31, 32, 33, 34], none of those references for the other applications discusses the probability of disruptive switching attack upon a compromised substation from the actuarial point of view.

A similar type of attack has been addressed as a cyber-physical switching or system reconfiguration attack [35, 36]. A compromise of the controllers for a generating unit is also categorized as a switching attack [37, 38]. The influence of such attacks reflecting grid vulnerability is clarified using the sliding mode trajectory [35, 36]. Such detection of anomalies can be achieved through game-theoretic analysis or the multiple-model inference algorithms [37, 38].

The recent research studies for cyber-physical switching attacks highlight a coordinated attack that consists of the false data injection attack, reconfiguration attack, and distributed denial of service (DDoS) attack. Considerable coordinated attacks are the plot against multiple component failures through a compromised network that connecting multiple components, such as lines or substations. With the coordination of the DDoS attack, there are combinations of attack scenarios that can be translated into false data injection attacks on wrong measurements of generators, lines, or loads.

It is common to relate bi-level modeling for the Load Redistribution (LR) attack, bi-level model for coordination of LR attack, and all sorts of other attacks [39]. Such strategies can lead to an optimal strategy with well-coordinated planning by attackers that can potentially weaken grid operating conditions [39].

Among those possible coordinated switching attacks, this dissertation focuses on the coordinated attack against substations because the impact of this type of cyberattack becomes larger than others (Table 1.1). It should be noted that this dissertation does not explicitly demonstrate the false data injection attack nor denial of information access. However, those are indirectly included in the proposed Petri net model as the probabilities, which will hereinafter be explicated. The first contribution of this dissertation is to elaborate on the steady-state probability for a cyber-physical attack at any IP-based substations, *i.e.*, the probability will converge over a long time upon successful intrusions to the internal networks.

Table 1.1
Substation component

Component	Connected component	Generation loss	Load loss
Power station	Power line Substation	High possibility	Low possibility
Transmission line	Power station Substation	High possibility	Low possibility
Substation	*Power station* *Power line* *Customer* *Var compensator*	*High possibility*	*High possibility*
Customer (load)	Power line Substation	Low possibility	High possibility
Var compensator	Substation	Low possibility	Low possibility

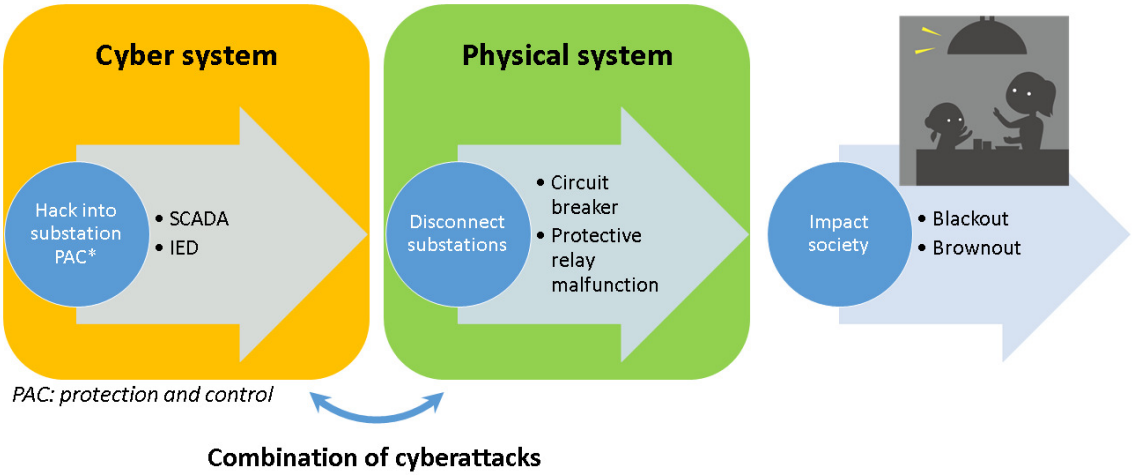


Figure 1.4: Coordinated cyberattacks and large-scale blackout

The hackers' main purpose is to make people trouble on a nation-wide level. Therefore, they spend time and energy to hack into substation systems first. Then, open multiple circuit breakers connected to the substation. If a customer's feeder is directly connected to the substation, that customer loses electricity. However, some substation attacks can cause cascaded failure (in other words, *domino effect*) in the power system. That means we eventually have a large-scale power outage (Fig. 1.4).

There are increasing cyber-related events in the "power system field" as well as other fields such as data breach news on social medias or famous credit companies. However, many power engineers believed that *cyberattack driven power outage* would not happen. The Ukraine's blackout in 2015 became a trigger to realize that cyberattacks actually cause a large-scale power outage (Table 1.2). The cyber-related events in power grids are rigorously showcased in [40].

Table 1.2
Cyber-related events in power systems

Date	Target and cyberattack type	Country
2003	A nuclear power plant	U.S.A.
Feb. 2011	A power plant management system	Brazil
2013-2014	Stuxnet-like attack (against over 1000 energy companies)	84 Counties
2014	A Large US Power Company's Automatic Voltage Regulator	U.S.A.
Dec. 2015	BlackEnergy malware attack against regional power companies*	Ukraine
Dec. 2016	Industroyer malware attack against regional power companies*	Ukraine
May 2017	Ransomware against India's West Bengal State Electricity Distribution Company	India
2017	Cyber attack petrochemical power plant	Saudi Arabia
2019	Power grid cyberattack in western interconnection	U.S.A.
2020	IT network of ENTSO-E	35 countries in EU

* cyberattacks that cause large-scale power outages

In light of this, power companies worldwide seemed to revisit the *cybersecurity reinforcement plan* in their power systems. unlikely to be proactive to invest in security matters without the government's requirement. The typical approach is to apply extrinsic motivations to power companies, establishing more strict cybersecurity standards with compliance tests (Fig. 1.5). However, facilitating their intrinsic motivations can also be a promising approach (Fig. 1.5). Then, the concept of the cyber-insurance framework emerges.

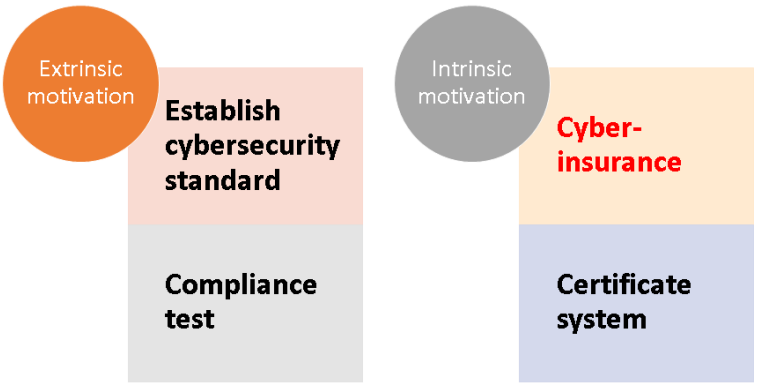


Figure 1.5: Extrinsic and intrinsic motivation for cybersecurity improvement

If we assume that the cyber-insurance framework is available, power companies can reduce the insurance premium. Once they showcase new advanced cybersecurity technologies, they improve the security level (Fig. 1.6). When the installation and operating costs for the new technologies meet with the premium saving, power companies can spontaneously employ the new cybersecurity technologies regardless of the standards. As such, the cyber-insurance framework can urge power companies to reinforce the cybersecurity level effectively. Besides, this framework can evolve cybersecurity standards even faster.

Although health insurance and car insurance are a widely known business, no cyber insurance of power grids is in not used. To establish a feasible cyber-insurance

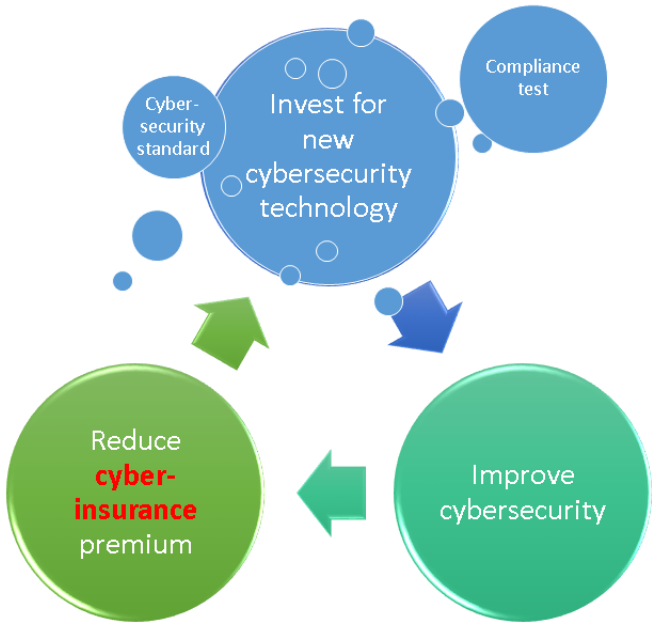


Figure 1.6: Mechanism of cybersecurity improvement with cyber-insurance framework

framework against power systems, the accurate estimation of the cyber-risk with its corresponding impact is mission-critical (Fig. 1.7). However, the risk analysis and the impact analysis of the cyber insurance framework are incredibly challenging and sill in infancy.

In the power grid's impact, electricity loss (or loss of electricity) is the most critical indicator because electricity loss is directly linked to economic loss/impact. As mentioned earlier, the cascaded events that are not from cyberattacks can additionally occur in the power system. The steady-state analysis does not always properly capture the process of the dynamic aspect of cascaded events. Therefore, dynamic simulations play a key role for the impact analysis.

As mentioned earlier, the first contribution of this work is developing a cyber-net

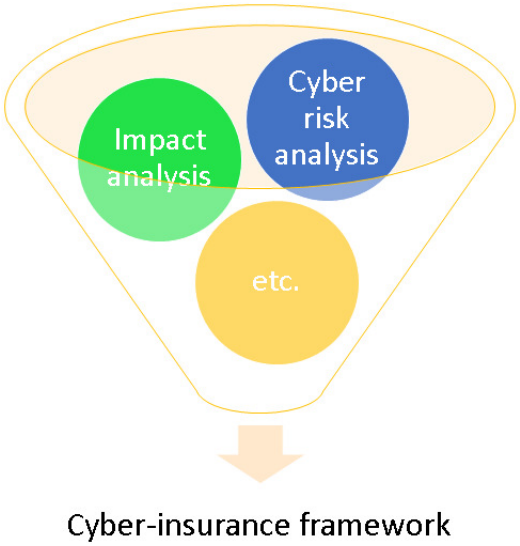


Figure 1.7: Mechanism of cybersecurity improvement with cyber-insurance framework

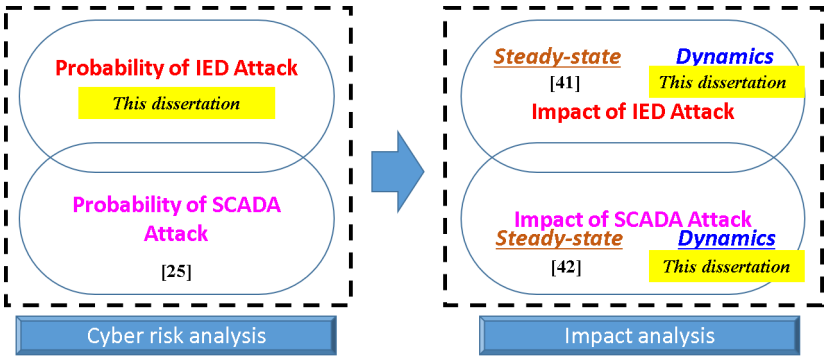


Figure 1.8: Contribution of this work

model that describes cyberattacks not only for the SCADA but also for IEDs (Fig. 1.8). The second contribution is to establish the analysis of substation attacks using a time-domain simulation tool instead of steady-state analysis [41, 42] (Fig. 1.8). The reviewed articles are related to coordinated cyberattacks and cyber-insurance in the power system.

1.2 Literature Review

Risk analysis and cyberattack: In the risk analysis, a way of intruding the control and protection system in the grid needs to be hypothesized. Among the enormous hacker's measures to intrude, the coordinated cyberattacks are extracted for rigorous review. Coordinated cyberattacks are known as the main reason for Ukraine's cyberattack in 2015 [43]. Since this incident, coordinated cyberattacks are the most significant concern for large-scale blackouts.

Impact analysis and electricity loss: In the power grid's impact, electricity loss (or loss of electricity) is the most critical indicator because electricity loss is directly linked to economic loss/impact. Then, approaches to the impact analysis for cyberattacks are exhaustively investigated.

Finally, the state-of-the-art research studies on the actuarial framework of cybersecurity on the power grid are reviewed.

Categorization Each article is intensively showcased, grouping them. The adopted categorization with its criteria is sorted out (Table 1.3).

In the first category, the automatic generation control (AGC) manipulates generators and indirectly affects customers. Disconnecting customers result in the power cut. The second category, protective relays, can cause the substation-wide outage. Because

Table 1.3
Categorication and its criteria

Categorization	Relevance of blackout	Relevance of coordinated attack	Relevance of actuarial framework	Number of articles
AGC	System-wide control system can disconnect some customers.	✓		3
Protective relay	Bus protection disconnects all components connected to a single substation.	✓		3
Sequential coordinated attack	Multiple disconnection of critical power equipment can cause blackouts.	✓		4
Actuarial framework	N/A		✓	4
Countermeasure for coordinated attack	Blackout scales can be different depending on the countermeasure.	✓	✓	3

both generators and loads (*i.e.*, customers) can be removed from the power system, the partial or whole blackout is inevitable. The third category, sequential attack, intentionally performs cascaded events, disconnecting critical power equipment one by one. The hacker's cascaded disconnection is highly likely to provoke the real cascaded events, which leads to blackouts. The fifth category assumes a certain level of the blackout to show the performance of the countermeasure. Therefore, this category is indirectly related to blackouts.

Paper selection: The IEEE publishes most of the reviewed articles. Eighteen papers are downloaded from the IEEE website, while two papers are from the Elsevier website. The selected papers were mostly published in the range of 2018-2020. The early access papers are proactively reviewed to catch up with state-of-the-art research studies.

1.2.1 Coordinated Effort in Plotting an Attack

A wide variety of combinations are leveraged for the coordinated attack studies. The fundamental concept is a mixture of an attack against physical electric components (e.g., transmission line, generator) and another attack against cyber components (e.g., generation control systems and SCADA systems). However, no paper had curated the patterns of coordinated cyberattacks.

Xiang *et al.* [44] performed the first attempt to overview the studied patterns of coordinated cyberattacks. Reference [44] analyzes the cyber-physical security in the grid to prevent future coordinated attacks against power systems and proposes probable coordinated attack scenarios. In light of the limited source about possible coordinated attack scenarios with detailed mathematical modeling, the authors highlight two typical attack coordination examples: the coordination between load redistribution (LR) attack and attacking generators; and the coordination between LR attack and attacking transmission lines. The bilevel optimization [45] formulates the two coordinated attacks. 1) At the upper level, hackers attempt to maximize load loss. 2) At the lower level, grid operators strive to minimize load loss. The case studies in a modified IEEE 14-bus system [46] demonstrate how coordinated attacks can potentially lead to a power outage. Also, it shows that coordinated attacks could cause a larger blackout scale than standalone attacks. This paper also provides beneficial tips for countermeasures on preventing and mitigating coordinated attacks based on those results. For example, protecting critical measurements or devices only works to mitigate the impact of the false data injection attack.

This article is extremely beneficial to get a big picture of the coordinated attack in the cyber-physical power system because different engineers have different coordinated attack patterns (Fig. 1.9). The authors listed up the possible combinations of the coordinated attack shown below:

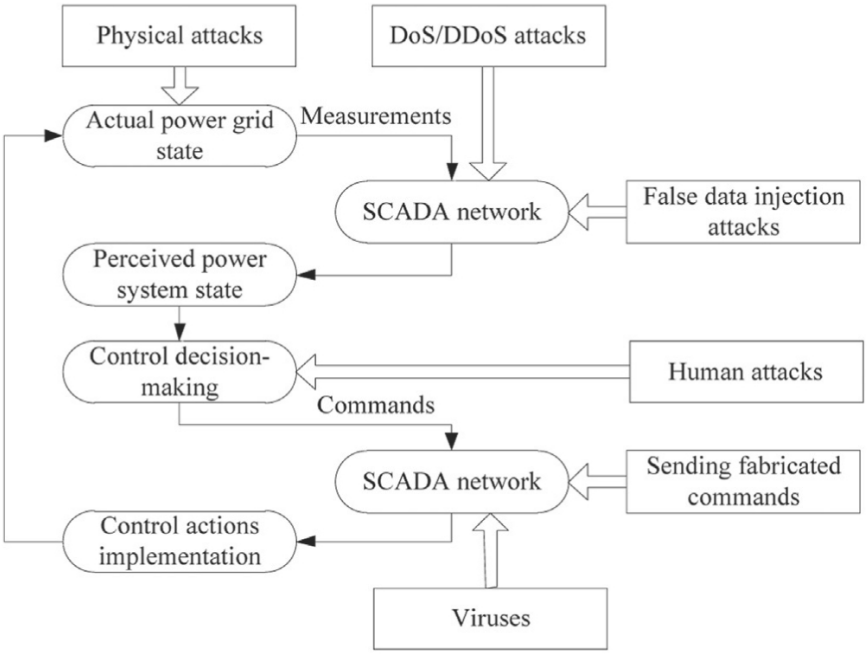


Figure 1.9: Power system operation and attacks [44]

- Multiple line attack
- Multiple substation attack
- Line attack with DDoS attack
- Generator attack with false data injection attack
- Line attack with changing relay settings (*i.e.*, with configuration change attack)
- Load redistribution (LR) attack with line attack

Despite the detailed review of the Ukraine cyberattacks at multiple substations, the coordinated attack that consists of the switching attack and the DDoS attack is out of scope in the case study. Besides, the employed power flow-based analysis passes over the power system dynamics, resulting in a large error when calculating electricity loss.

1.2.2 Deceiving the control of AGC

The automatic generation control (AGC) is a grid-wide control system that can significantly impact the whole interconnected grid. Among the reviewed papers, three scholarly articles study the coordinated cyberattack against the AGC.

Article 1: Liu and Wang [47] face the cybersecurity issue with the internal threat. Reference [47] studies the load redistribution attack with insider threats to combat the cyberattack associated with the data breach (*i.e.*, the data integrity attack). The studied insider threat is the information leakage of the system operator's defense strategy. The leaked information is assumed to be acquired by the intruder and leveraged by other attackers. The proposed "security resource allocation" game model formulates the insider's information leakage and maximizes the operator and the attacker's rewards. The IEEE 14-bus and 118 bus systems' case studies indicate the system operator's defense action's severity to mitigate the load redistribution attack. Moreover, the case study provides the following useful insights to grasp the data breach's impact on the steady-state condition. 1) The information leakage of the defense strategy provides a significant advantage to attackers, increasing the expected reward, especially before operators notice the data breach. 2) The damage on the grid can be enormous even by the subtle data breach. The operators' reward analysis also clarifies that an increase in the security resource can be a cybersecurity measure

to alleviate the insider threat's LR attacks.

The authors achieved great success that the attacker and operator's mixed strategies at the Nash Equilibrium of the game enable us to formulate and solve the minimax (or min-max) problem. However, the aforementioned two insights can be easily anticipated qualitatively without case studies. Moreover, the leaked data is energy consumption only. Therefore, the contribution is somehow limited. Reference [44] contrasts the impact of LR attacks with and without AGC/LFC information. To offer better findings to readers, the authors should elaborate more on the sensitivity analysis considering a wide variety of data breach types.

Article 2: Chen *et al.* [48] examine the impact of the load redistribution (LR) attack against the load frequency control (LFC) system with the load (manipulation) attack to elaborate more on the combined attack's impact. The authors maximize the combined attack's impact in terms of the minimum cost (least-effort attack) perspective and the maximum power imbalance (maximizing frequency disruption via a change in generation and loads) perspective, respectively. Also, they contrast the impact with and without the availability of the LFC system information. The proposed optimal coordinated attack scheme consists of the critical load bus identification for the load manipulation and the optimal attack sequence design. A developed prevention measure is based on the proposed optimal cyberattack scenarios with newly proposed threshold-based detection methods. The case studies provide two new findings.

1) cyberattack performances incredibly vary with different attack objectives (as the time to the frequency violation decreases, the attack cost exponentially increases); 2) the proposed threshold-based detection methods to cope with the coordinated attack can screen out the compromised signals.

This article presents an exceptional work, clarifying the remaining work in the LR attack topic. Compromising the LFC can fluctuate the system frequency broadly. However, it is unlikely to cause blackouts unless all loads are manipulated. The authors set 0.5 Hz as the frequency excursion level, which is not controversial because such threshold values vary depending on countries and grid size. However, LFC is not only the frequency control in the power grid. We also need to consider the emergency control that stabilizes the grid frequency stability. Therefore, the derived impact through the simulation study is not accurate enough (*i.e.*, it is not realistic).

Article 3: Fu *et al.* [49] yield a sequential coordinated attack framework for the power grid to analyze the cyber risk against the combination of the switching attack over the transmission lines and the load redistribution (LR) attack (or false data injection attack) for the automatic generation control (AGC) system. The cascaded line tripping model based on the Oak Ridge-Pserc-Alaska (OPA) model [50] represents the sequence of cyberattacks (*i.e.*, line tripping attacks). The well-known bilevel model emulates the LR attack. The objective function and constraints of the model are modified to obtain severer cascaded failure with power outages. The Q-learning

based solution algorithm that the authors employ identifies the severest sequential coordinated attack scenario. According to the simulation study with the IEEE 39-bus system [51, 52], the proposed sequential coordinated attack tends to cause more extensive power outage than the line tripping attack only due to evolving cascaded events.

The novelty of this article is to copes with the three things simultaneously: 1) A physical attack (transmission line tripping), 2) A cyber attack (load redistribution attack delivering the false control signal to the generation dispatching control system), 3) A sequence of attacks (line tripping events). However, the physical attack is not always the transmission line outage, but transformer outages and generator outages. Also, cascaded events toward power outages are analyzed using only a power flow-based approach. In other words, the dynamic behavior in the power grid during the cascaded event is ignored.

Impact indicator in 3 articles In terms of the impact of the hypothesized coordinated cyberattack, [47] considers only steady-state conditions without the impact of cascaded events. In other words, the difference between the economic dispatch and the load tripping cost is treated as the economic loss along with the operational loss and load loss. Reference [48] determines the whole system collapse using a threshold value of the frequency level. Reference [49] accounts for the number of separate lines as the impact. Only [48] deals with electricity loss as the impact indicator. Overall,

compromising only the AGC is unlikely to cause a large-scale power outage.

1.2.3 Manipulating the Protective Relays

Protections play an essential role in isolating targeted power equipment to prevent it from damage. That means protective relays disconnect the power equipment from the power system. Such power equipment loss can be a trigger of electricity loss along with cascaded events. Among reviewed papers, three articles cover this topic of compromising relays.

Article 1: Hong *et al.* [53] present an ICT layer-based and power grid domain-based mitigation method to detect and alleviate cyberattacks on substation automation systems. The developed mitigation method tackles the hacker's malicious action on opening circuit breakers (CBs) via a configuration change attack (by changing line protection settings), sensor data injection attack, and a direct CB control attack. The established protection coordination cross-checks principle detects the configuration change attack. The proposed transient fault signature-based cross-correlation coefficient algorithm points out the false sampled values data injection attack. The power grid-domain-based mitigation method clarifies the impact of nuisance CB operation (mainly overloading) before its action to obviate potential cascading failures due to a human error. The hypothesized intrusion scenario to the digital substation

is emulated in a testbed (consisting of a HIL simulation with commercially available IEDs and an RTDS) to validate the proposed substation attack mitigation method's performance. The proposed method showed excellent performance.

Although this article demonstrates the promising anti-cyber attack functionalities, only one type of protection and communication protocol is studied. In other words, the developed method's verification is limited to a single component level, not the system-wide level. For instance, the coordinated attack on multiple IEDs is treated as future work. Besides, the cybersecurity level improvement is mostly qualitatively explained. For example, the blackout scale caused by the malicious CB operation is not quantitatively clarified. Although the authors use the testbed for the validation, the justification of the proposed method is limited.

Article 2: Khaw *et al.* [54] describe a deep learning-based anomaly detection system to protect distance protections from false tripping cyberattacks to protect the power grid from potential cascaded failure. The authors tackle the following three cyberattack scenarios. 1) false data injection attack, 2) replay attack, 3) integrity attack via relay tap manipulation. The time-domain simulation with a wide variety of loading levels of generators and fault locations is used to train the autoencoder via the deep-learning algorithm [55]. The applied fault type is a three-phase fault only. The trained autoencoder can identify the malicious data (*i.e.*, voltage, and current), mitigating the false data injection attack. The case studies exhibit 100% accuracy

against the false data injection attack and relay tap manipulation attack. On the other hand, the technical challenge remains for the replay attack.

This article adopts an anomaly detection approach instead of a misuse detection approach, taking into account the stealthy nature of cyberattacks in the power grid. Because the fault characteristics are highly likely to change due to the increasing penetration of renewable energies, the anomaly detection approach must be more promising. Although the undertaking technical challenge has similarities to [53], the replay attack is newly studied. However, as mentioned in the article, only a balanced fault is considered for the training datasets. Because over half of the fault type across the globe is the single-line-to-ground fault, the authors should cover the unbalanced fault. Besides, the tap position change is highly unlikely to happen while using it, according to my best knowledge. The system operators usually change the tap position only when that relay is out of service. Therefore, relays must be equipped with an interlocking function so that tap positions cannot change under an operating condition. Therefore, the relay tap manipulation attack may be out of scope.

Article 3: Chattopadhyay *et al.* [56] reveal the impact of an implementation attack on substations to highlight the substations' security analysis gap. The authors provide an overview of potential exploits clarifying security issues and dominant attacks against IEDs and substations. The differential power analysis, voltage/frequency scaling, fault injection, and malware attacks are significant concerns for IEDs. In

contrast, GPS spoofing, Ethernet switch attack, SCADA attack, and WLAN attack are the concern for substations. The authors perform two detailed case studies on malicious false injection attack and hardware attack. The instruction attack is clarified as the typical false injection attack with low-cost. Two possible countermeasures are exhibited with the pros and cons. The first one, with instruction redundancy, delays the reaction time but avoid increasing the cost of IEDs. On the other hand, the second one that requires an additional sensor increases the cost but keep the reaction time within the permissible range. The authors emphasize the difficulty in protection against the hardware attack because such an attack is designed to be dormant, causing slow degradation of the relay performance.

This article is incredibly informative and provides much practical and fruitful information not only for relay engineers but also for cybersecurity engineers. Unlike standard journal papers, the novelty and creativity of this article are subtle. However, the authors show off professional knowledge as a relay engineer with plenty of observation of the attack process against the protective relay in-depth. Although this article covers the cyberattack's impact on the substation level, most discussions are limited to the IED level. Therefore, this article falls short of elaborating on the impact on substations, especially the process of spreading influence.

Impact indicator in 3 articles All three references develop a mitigation approach that directly or indirectly detects malicious action and blocks the false tripping. Reference [53] prevents a substation (automation) from:

- Configuration change attack (to change relay settings),
- False data injection attack (to change measured data),
- Switching attack (to operate circuit breakers),

while [54] prevents a distance relay from:

- False data injection attack (to change measured data),
- Replay attack (to change fault characteristics),
- Integrity attack (to change relay taps).

Reference [56] discusses hardware attacks as well as the false injection attack. No articles deal with the impact on the power grid, mainly because establishing the effective mitigation method is the most significant interest in those researches. It should be emphasized that no research on wide-area protection is studied in terms of cybersecurity.

1.2.4 Sequential Attack

Sequential attack events often cause large-scale blackouts along with cascaded grid events. Among the reviewed papers, four scholarly articles study the sequential coordinated cyberattack. It is noted that [49] also covers the cyberattack against the transmission line.

Article 1: Paul *et al.* [57] analyze the impact of the sequence of cyberattacks on the blackout scale, examining the learning parameters of cyberattack strategies for combating the hackers on the energy sectors. Authors adopt the learning-based game-theoretic approach [58] with the multistage sequential game to interpret the dynamic sequence of events and determine the worst cyberattack scenario and the most effective defense policy. A commercially available time-domain simulation tool, named Power World simulator, reproduce the learned cyberattack scenario, illustrating how the switching action (*i.e.*, disconnecting transmission lines one by one) disrupts the grid operation accompanying the voltage violation, frequency violation, and overloading. This paper serves as a case study in the IEEE 39-bus system [51, 52] that proved that the learning process improves the defense strategy. The obtained new findings can make the grid security more robust and reliable against the cyberattack.

To my best knowledge, this article is the only source to demonstrate the time-domain

simulation results for the sequential cyberattack. Because the used models are a dynamic simulation model of the Power World simulator, the synchronous generator's obtained dynamic behavior during the cascaded events is sufficiently accurate. On the other hand, the protective relays, such as over frequency protections, are not modeled. Therefore, other dynamics caused by protection operations are missing in this paper. Also, the switching action targets are limited to line tripping. However, transformer outages and generator outages can have a more significant impact on power system stability.

Article 2: Zhang *et al.* [59] evaluate sequential cyber-topological attacks on cyber-physical systems to figure out the critical sequence of cyberattacks that can lead to cascading outage. The studied sequential attack is a coordinated intrusion attack to grid branches with the false command injection attack and distributed denial of service attack. An established coordinated attack process clarifies a mechanism with a probability analysis considering the different timescales. The used tree-layout Markov decision process model illustrates the cyberattack patterns/sequences, assisting in identifying the minimal attack sequences that cause blackouts. The proposed pattern concept that consists of critical combinations of attack events significantly compresses the storage of risky attack sequences. The established search strategy dynamically selects the next attack target, gradually increasing the search depth, which reduced the heavy computation burden. The AC power flow-based case study in the IEEE

39-bus system [51, 52] exhibits the proposed strategy's outstanding performance with the successful extraction of representative attack patterns.

This article provides a clue as to reducing the exhaustive enumeration of attack scenarios. Therefore, the proposed scheme is beneficial only when we take a wild guess using the power flow-based approach. However, the actual cyber-physical system contains power system dynamics. For example, the rotor dynamics of synchronous generators, various voltage and frequency controllers' responses in the grid, and a wide variety of protective relay operations significantly affect the load loss scale. Without those dynamic aspects, we cannot correctly represent the real power system behavior during cascading outages. In other words, the power flow-based wild guess of the load loss includes an enormous error.

Article 3: Wang *et al.* [60] mine frequent attack patterns consisting of cyber attack sequences and physical attack events to estimate the hacker's attack process on the entire electric power cyber-physical system (CPS). The authors define a coordinated attack as a mixture of cyber and physical attacks, assuming that the cyberattack always comes first. The fuzzy C-means clustering algorithm extracts the cyber-related events from the collected alarm logs. The developed algorithm based on the temporal-causal Bayesian network [61] recognizes the cyberattack sequences. The combination of physical attack event criteria algorithm detects the physical attack events using the characteristic curves of different attack measurement data in physical space. The

proposed coordinated network attack sequential pattern mining algorithm with the frequent pattern tree finds out the hidden multi-step attack patterns as well as the frequent patterns of attack sequences. The testbed to which the established method was implemented proved that the cyber-physical attack was tracked effectively and efficiently.

The authors did fantastic work to reveal the attack process in cyber and physical spaces. The developed temporal-topological correlation-based algorithm successfully improves the validity of the entire cyber-physical attack. No prior knowledge to create the rules associated with the method enables us to be practical use more smoothly. However, the detection algorithm against the physical attack remains room to be improved because we cannot differentiate between the three situations regardless of using the temporal-topological correlation: 1) abnormal phenomena caused by hackers, 2) abnormal phenomena caused by power equipment failure, measurement device failure, and communication equipment failure, 3) abnormal phenomena caused by the power engineer's manipulation of the equipment during its maintenance.

Article 4: Sun *et al.* [62] develop a coordinated cyberattacks detection system on the grid to overcome the coordinated attack that the existing measure cannot resolve. The coordinated cyberattack here is the sequential (multiple) substation attacks. The developed detection system identifies relations among abnormal behavior patterns (e.g., intrusion detection system alarms, firewall logs), geography data

(e.g., geographic attack location), and substations' criticality. The created "time failure propagation graph" model with the "Fuzzy cognitive map" model calculates the state value in each phase of the attack process. The developed system (CCADS) delivers an alarm when the state value mentioned above continuously increases, informing the coordinated cyberattack in the designated grid. The simulation using a cyber-physical security testbed validates the online applicability for the proposed CCADS. The proposed CCADS can be used for the online detection of a cyber attack. The authors address the room to improve the detection efficiency and response time for real-time operation.

This article runs the time-domain simulation using a commercially available tool named DIgSILENT that has been widely used in power companies in the EU. Therefore, the dynamic behavior caused by the sequence of the hacker's disruptive switching actions can be demonstrated more accurately compared to many other research studies. However, this article does not cover the grid side resilience (*i.e.*, system protection, or SPS). For example, in low voltage/frequency, the undervoltage or underfreuqency load shedding system activates to take corrective actions, recovering the grid stability. Such systems are called remedial action schemes and are widely used in most of the advanced countries. Therefore, grid self-healing capability is missing, which results in the pessimistic result in this article.

Impact indicator in 4 articles Pertaining impact of the coordinated cyberattack, only [57] addresses electricity loss in the entire system. The rest three articles mainly pursue shortening the time to detect anomaly status [62] or critical attack patterns [59, 60].

1.2.5 Countermeasures Against Sophisticated Attacks

The following four articles deal with the countermeasure for coordinated cyberattacks. The first two papers aim to strengthen the resilience against cyberattacks. The rest two papers invent the mitigation strategy to contain the influence of cyberattacks on the power grid.

Article 1: Liu and Wang [63] create a grid topology optimization scheme to enhance the power system resilience against cyber-physical attacks, *i.e.*, coordinated attacks. The cyberattack here covers the switching attack on power stations and substations. In contrast, the physical attack denotes immobilizing transmission lines (via a transmission tower collapse, for example). A developed bi-level optimization model formulates the coordinated cyber-physical attacks against the power grids decomposing the upper level for the attack and the lower level for the grid recovery. A developed networked topology optimization (NTO) model [64] mitigates the cyber-physical attacks and strengthens the power systems' resilience. Case studies in the

modified IEEE 57-bus [65] and 118-bus systems [66] illustrate the impacts of coordinated cyber-physical attacks, validating the proposed NTO approach. The three resilience indicators (comprising a competence of electricity supply against a cyber-attack, the same competence from the attack event to the full grid recovery, the grid recovery time) proved that the proposed NTO-based mitigation strategy effectively reduced the total load loss caused by the coordinated cyber-physical attacks. The case studies also justified that decreased load loss and grid recovery time are smaller than those derived by the conventional two methods, *i.e.*, optimal re-dispatch and optimal transmission switching based methods.

To my best knowledge, the transmission tower collapse by a human attack happened only once in Japan over the last fifty years. The probability of such a physical attack is extremely low. On the other hand, the cyberattack on power stations and substations are highly likely to increase. The assumed combination of the coordinated attack is getting more unrealistic, especially in the future. Besides, the proposed strategy may be applied only for the breaker-and-a-half configuration busbar. Although the authors insist that this busbar structure is widely used globally, this structure is not dominant in many countries due to the larger space and higher cost. Therefore, the applicable grid must be quite limited.

Article 2: Touhiduzzaman *et al.* [67] determine the optimal allocation of the security mechanism diversity that minimizes security vulnerabilities to the grid to protect

the power system against coordinated substation attacks. The authors hypothesize the zero-day attack compromising the substation control system and disconnecting the targeted substations when the security hole remains before updating the software packages. The authors create a security graph model to represent the hacking process to substations in the cyber system. The threat model [68] disconnects substations via a zero-day attack. The physical system model [25] exhibits the loss of electricity, *i.e.*, power outage scale for each substation attack. The game-theoretic graph coloring technique [69] optimizes the deployment of software packages from cybersecurity perspectives. The case study exhibits how the diversity strategy reduces the risk of substation cyberattacks using the IEEE-118 bus system [66] as well as the IEEE-14 [46] bus system.

Although this work successfully shows the importance of proper diversity strategy to mitigate substation cyberattacks' risk, the assumed impact after hacking substations is represented as the load loss for the designated substation attack. The hacking probabilities are borrowed from another source [25]. Because [25] employs the power flow-based approach to derive the blackout size, the dynamic aspect during the cascaded failure/event is missing. This article addresses that a diversity strategy includes diversifying relay manufacturers. However, we cannot fully consider this action's effect because diversifying relay manufacturers can decrease electricity loss for the same substation attack.

Article 3: Li *et al.* [70] explore the vulnerability of a coordinated cyber-physical attack on the power grid to establish a countermeasure protection strategy within the constrained budget. The coordinated attack here comprises a physical and a cyber one. The first attack denotes the line disconnection. The second attack consists of the load (redistribution) attack and topology preserving attack. The second one masks the line event to evolve the deterioration of grid stability. The proposed new sensitivity factor, named generalized generation shift factor, depicts the sensitivity of power flow over the line to the bus injection. This sensitivity is used to derive the cyberattak's impact. The bi-level "mixed-integer linear programming" [71] formulation successfully identifies the most disruptive and invisible physical attack under the designated constraint. The case study indicates that a well-coordinated physical attack poses the topology-preserving attack, which incurs the severest grid impact. It is noted that the heavy computation burden for the use of the bi-level model, pointing out the increasing difficulty in applying the proposed approach for the larger grid. The authors also address that the offered protection strategy remains the technical challenge, although establishing the strategy per se is the final goal.

This article combats a challenging topic that has never been attempted. However, the employed severity indicator of the coordinated attack is the power flow over the transmission line only. Then, the authors discuss the overloading level. All transmission lines have a short-term rating and long-term rating. Whether the overloaded line is an issue depends on how long it takes to resolve the overloading condition via the

configuration change. The different loading level of the unit brings to a different time to complete the required configuration change. Therefore, so many essential system constraints are missing in this article. Besides, the authors use the wrong language for the "load redistribution." The meaning of "load" here is a generator's load, not the customer's energy consumption. Such misuse can incur the reader's misconception.

Article 4: Lakshminarayana *et al.* [72] devise a moving-target defense strategy to combat the coordinated cyber-physical attack in the power grid. The studied coordinated attack comprises the false data injection attack to provoke a physical disturbance and the concealment of the false data to have grid operators not recognized. The core of the moving-target defense strategy is to oscillate the transmission line reactances via distributedly deployed flexible AC transmission system (D-FACTS) devices all the time. Hackers cannot get to know the perturbed impedance before/-during the attack process. Therefore, the proposed moving-target defense scheme can detect the cyberattack, confirming no perturbed aspect in the measured data. The authors design the moving-target defense using two steps. 1) The graph theory derives the minimum subset of links for the D-FACT device deployment that covers attacks against all edges. 2) The game-theory identifies the best subset of links (within the D-FACTS deployment set) to perturb the grid minimizing the defense cost. The simulation case study in the IEEE 14-bus systems [46] provides the right perspective on the proposed moving-target defense strategy's detection performance

and cost performance.

This article copes with a new type of combined cyberattack, *i.e.*, to conceal the false data injection attack's signature. Therefore, the novelty lies in the tackled topic. However, generally speaking, the power system operator and engineers cannot accept injecting any perturbing signal at a grid-wide level. The main reason is that such fluctuated signals caused unwanted power swing oscillation in history. Such oscillation can also jeopardize the performance of the current protective relay performance. Therefore, the proposed strategy is significantly unrealistic because it leads to the power system operator's growing concern about deteriorating grid stability.

1.2.6 Definition of Coordinated Attack

The generalization of a coordinated cyberattack is a combination of multiple attack tactics. However, many engineers across the globe have defined the same term in a different way. Substation switching attack is one example of a typical coordinated attack due to the compromised control system in a substation by a bad actor in the cyber system, and circuit breakers are presumably manipulated (tripped). The coordinated attack in this dissertation denotes a manipulation of switching sequence through the compromised control system in substations.

1.2.7 Actuarial Framework

The following four scholarly articles cover the actuarial framework in the power system. The first three are relevant to cyberattacks, while the last one does not pertain cyberattacks.

Article 1: Liu *et al.* [73] invent an actuarial framework to capture and reduce the hazardous nature of interdependence among cyber risks, intending to enhance the cyber insurance market for power systems. The authors research the insurance schemes for power systems against emerging cyber threats. The absorbing semi-Markov process models the cyberattack scenarios on the power grid. Besides, a developed stochastic model reflects the correlation of cyber risks across the power system. A created sequential Monte Carlo simulations framework evaluates the power grid's impact not only by physical component failures but malicious cyberattacks. This article then designs an insurance scheme to manage the power grid's risks with the financial consequences against cyber threats. The case study with the proposed premium principle reveals the significant impact of self-protection in cybersecurity. That can drive stakeholders to invest further in cybersecurity. Therefore, the presented actuarial framework is highly likely to enhance the participation rate from insured parties as well as insurers' perspectives.

The authors combat an unprecedented problem in establishing actuarial frameworks against cyberattacks in the bulk power system and obtains beneficial new findings. However, this paper showcases one optimistic assumption and one pessimistic approach. The first one is that hacker's disconnecting power equipment always succeeds. The second one is that cascaded events toward power outages are analyzed using only a power flow-based approach. In other words, the dynamic behavior in the power grid during the cascaded event is ignored.

Article 2: Yang *et al.* [74] establish a cyber insurance premium calculation framework regarding cyber risks in digital substations to establish a new cyber insurance business in the power system field. The assumed cyberattack here is substation attacks via hacking the SCADA system. The proposed cyber insurance framework comprises three components: 1) the power loss caused by the hypothesized substation attack, 2) the grid restoration time after the outage, 3) the blackout scale-dependent economic loss. The employed ruin theory [75] determines the feasible insurance premium pool using the aforementioned three elements. The authors simulate massive substation attacks in the IEEE test systems with the power flow software to obtain the brownout/blackout scale. Then, they derive the grid restoration time as the "mean time to restore power" using the generic restoration milestone model. The economic loss is borrowed from a publicly available source such as the ERCOT report [32]. Sensitivity analysis and spatial correlation study results provide findings. For

example, the unit's ramp speed and the loading level give a more considerable impact on the "mean time to restore power."

This article describes a new idea of how to calculate the cyber insurance premium in the power system. Although the overall approach with the cyber attack target is similar to [73], only this article explicitly considers grid restoration time for the calculation. The probability of hacking the SCADA system is represented as steady-state probabilities, the data of which are referenced from other sources (e.g., [25]). Because [25] employs the power flow-based approach to derive the brownout/blackout scale, the cascading event's dynamic behavior is missing. Besides, the case studies are nothing to do with the importance of cybersecurity-enhancing measures, such as the honeypot. One of the grid's cyber insurance contributions is to let grid companies invest in cybersecurity technologies more appropriately and proactively. Therefore, the comparison study for the insurance premium with and without upgrading cyber-security strategy is preferable.

Article 3: Lau *et al.* [76] design a new actuarial principle to estimate each transmission company's premium, considering correlated cybersecurity risks and the balance between the security investment and saving in the insurance premium. The developed Stakerberg Security Game model [77] formulates the optimal mixed strategies and deploys the defense resources across multiple targeted substations, representing the optimal stochastic distribution mechanism. The created Semi-Markov Process model

[78] derives the intrusion tolerant competence in the SCADA system that buffers residence time before the substation outage to enhance the grid resilience against cyberattacks. Case studies obtain the above competence for various attack scenarios with findings. 1) The self-resilience against the substation attack in SCADA systems depends on the defense resource allocation. 2) The more defense resources are invested in the substations, the more intrusion tolerant capability against substation attack can be enhanced. 3) The designed insurance premium principle can provide the incentive for investments in enhancing the intrusion tolerance capability.

This article tackles a non-business matter, *i.e.*, cyber insurance in power grids. The authors claim that cyber buying insurance in power grids is likely to be mandatory in the future. However, many challenges remain. For example, grids are electrically connected and tightly interrelated. Therefore, the cybersecurity investment in one power company affects the security level in other companies. If the insurance premium decreases for one company only, this raises a fairness issue. This article assumes only one company in the entire grid. That means the proposed scheme may be leveraged only in an isolated grid or the grid with no AC interconnections, such as Japan and ERCOT in the U.S.

Article 4: Yang *et al.* [79] advance an insurance strategy to offset the possible imbalance cost that wind generation owners need to bear due to the intermittent power

output. The authors assume that wind owners participate in the electricity market. The energy storage system (ESS) selected as an alternative approach alleviates the supply-demand imbalance caused by inaccurate wind forecasts. The insurance compensates for the residual loss. The ESS and insurance policies are combined to reduce the imbalance risks of trading wind power as a whole in real-time markets. The proposed approach determines the most economical ESS capacity in different excess scenarios. The Monte Carlo simulation estimates the insurance premiums, analyzing the impacts of insurance excesses on premiums. Case studies indicate that the proposed insurance strategy is likely to achieve the risk aversion with the ESS against the trading wind power in real-time electricity markets.

This article addresses that insurance in the power grid has tremendous potential as a risk transfer tool. In other words, the insurance business may be enhanced to the power system field, which means we can extend the actuarial research to cybersecurity. Although this article demonstrates the outstanding preliminary results, many other things need to be considered to substantialize. For example, the minimum battery capacity can tremendously differ depending on the controller (e.g., active power control and state of charge control) and the battery type (e.g., sodium-sulfur, lithium-ion, vanadium redox). Besides, the proper control to minimize the battery capacity also depends on the wind power property (e.g., the power output characteristics vary depending on the number of blades).

Common research purpose in 4 articles Reference [74] performs the first attempt to showcase a sound approach to derive the insurance premium for the cyber related event in the power system. On the other hand, the rest three scholarly articles more focus on advancing an idea to incentivize the grid owner for reinforcing cybersecurity.

1.3 Critical Research Areas in Wide-Ranging Attacks

Recommended research areas for a great variety of attack plots is asserted in one of the reviewed articles.

Ni *et al.* [80] do not directly study the coordinated cyberattacks but propose a concept of cyber-physical "coordinated situation awareness." They also propose an active defense against cyberattacks based on the temporal and spatial correlations between cyber and physical systems to overcome the limitation of the conventional one-sided defense system. The employed example regional frequency control system validates the proposed concept, representing the overall theoretical architecture and the key technologies. The proposed concept comprises two actions: 1) coordinated situation

prediction and early warning, 2) coordinated trace-back of cyberattacks. The coordinated trace-back consists of the faulty device identification at the physical system and the attack traceability at the cyber system. The authors clarify the following critical research areas to implement the coordination and reap the corresponding benefits rigorously.

1) Cyber-physical power system (CPPS) and cyberattack modeling,
2) Analysis of CPPS security,
3) Risk analysis considering anomaly attacks,
4) CPPS control theory.

Lastly, the authors recommend the importance of collaborative work between the cyber and physical planning divisions to pursue the optimal control and planning for the CPPS.

This article provides tailored research challenges toward the coordinated cyberattack in the cyber-physical power grid. Despite less novelty, the authors did fantastic work with sufficient creativity, providing an integrated view of the field's research activity. Although the page limitation restrains the covered topic, the authors should investigate and discuss not only the frequency control system but also the voltage control system in terms of the applicability of the proposed concept. This dissertation covers the aforementioned research areas and contributes to the above 1) and 2).

1.4 Security Threats Against Power Communication Infrastructure

1.4.1 Targeted Facilities in Power Grid

Nowadays, more engineers gain their interest in a research study on cybersecurity against power grids. According to the literature survey in Subsection 1.2, the targeted power equipment is shown below:

- Generator (power station, AGC)
- Transmission line
- Transformer
- Customer (load)
- Digital protective relay (IED)
- Substation

The first four equipment is a representative component of the power grid. On the other hand, substations cover all four components mentioned above. Protective relays are deployed at power stations and substations to protect the above four components from disturbances, such as lightning strokes. Although relays are one type of equipment,

they do not play the role of generating, delivering or consuming electricity. The AGC is a grid-wide control system that is different from others. Because the load redistribution (LR) attack is a well-known term among cybersecurity experts, the term, LR attack, is often used instead of addressing the cyberattack against AGC. Other than the aforementioned list of power equipment, local voltage controllers are also a target of cyberattacks, such as SVC/STATCOM[81, 82, 83], and AVR[84]. Also, wide-area monitoring, protection, and control systems (WAMPAC[85], also known as SPS and SIPS) target cyberattacks (especially the DoS attack) [86, 87, 88, 89]. Among those targeted power equipment, the substation attack attains the highest research interest in this research field (Fig. 1.10). This dissertation focuses on the substation attack, including the power station attack. It is noted that the electricity market is also a target of cyberattack [90, 91, 92, 93], although it is not the power equipment.

1.4.2 Attackers' Stratagem

Cyberattacks are categorized into several types of attacks. According to the literature survey, the following eight cyberattacks are studied (Table 1.4).

Among those types of cyberattacks, the switching attack attains the highest research interest in this research field. Targets of the switching attack are mainly substations or power stations. Three articles cover opening transmission lines as the switching

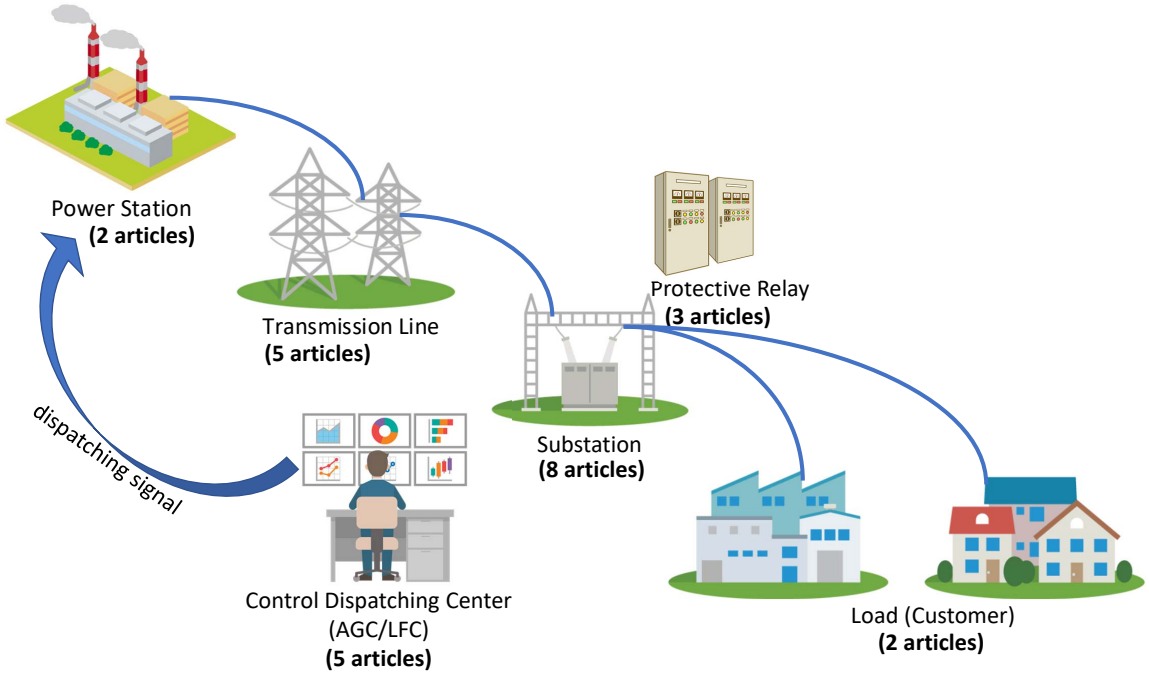


Figure 1.10: Targeted facility in power grids

Table 1.4
Type of cyberattack and corresponding target

Type of attack	Target	Number of articles
Data integrity attack	Load	2
False (data/command) injection attack	Relay, CB	4
Configuration change attack	Line, Protective Relay	4
Distributed DoS attack	AGC, CB	2
Load redistribution (LR) attack	AGC	3
Switching attack	Line, substation, power station	10
Replay attack	Protective Relay	1
Zero-day attack	Software in substation	1

attack. Because this dissertation focuses on the switching attack against substations, including power stations, the central research topic is in the scope of the dissertation.

On the contrary, the DoS attack is the most predominant type of cyberattack. For

example, the DoS attack on the Internet exhibited a 16% increase in the first half of 2018 compared to the same period in 2017 [94]. This fact boosts up this research study of DoS especially for AMI [95, 96, 97, 98, 99, 100, 101, 102]. It is noted that the distributed DoS attack is a DoS attack caused by multiple computers, while a single computer causes the DoS attack. The type of cyberattacks is not limited to the above list. For example, de-synchronization attacks [103, 104, 105, 106, 107, 108, 109, 110, 111] can be leveraged as another kind of DoS attack.

1.5 Doctoral Contributions

Risk analysis using steady-state probability of compromising SCADA and relays: Many of the recent research studies gain their interest in compromising the power system-wide control such as the AGC and the SCADA. "what-if" scenarios is mostly established, and many authors focus on validating the advanced counter-measure against cyberattacks. However, actuarial frameworks require the discussion on how often an event happens from stochastic power of view. The recent articles do not deal with this stochastic process but rather spend more energy on "what-if" approaches. This dissertation addresses the hacking process into the SCADA and IEDs (*i.e.*, protective relays) that cause disruptive switching actions on substations in a stochastic manner. This work refines the previous study [25], integrating new cybersecurity technologies such as two-step authentication and honeynet.

Impact analysis using power system dynamic simulation model: Almost all recent research studies adopt a static based approach, *i.e.*, power flow calculation program-based approach. Although more engineers have increased their interest in representing cascaded events/attacks, most approaches leverage the continuous, multiple power flow snapshots. Only a few engineers [57, 62] start to use the time-domain dynamic simulation program. However, they do not keep an eye on the cascaded events caused by system-wide protections. The significant challenge is no generally accepted guideline for the protection (relay) model selection. The relay settings are not always fully available. This dissertation serves as guidance on which relay models are required to represent the cascaded events. Besides, it demonstrates how the impact of cyberattacks becomes pessimistic when the power flow approach is employed instead of the dynamic simulation.

The organization of the thesis is organized as follows. Chapter 2 advances a cyber-net model that comprises cybersecurity technologies such as firewalls, passwords, two-step authentications, and honeynets to derive the intrusion probability as the stationary stochastic process. Chapter 3 presents the sensitivity analysis of case studies with discussions of security technologies that affect the steady-state probabilities. Chapter 4 clarifies the necessary dynamic control and protection models to demonstrate cascaded events that are stemmed from cyberattacks, with substation attack case studies. Chapter 5 concludes the dissertation.

1.6 Publication Listing

The following lists are published during the doctorate candidacy since 2012 while Mr. Yamashita was a part-time PhD candidate; he had been a full-time research at Central Research Institute of Electric Power Industry (CRIEPI). Koji converted his candidacy into a full-time PhD student at Michigan Tech in Summer 2018 and moved to the United States. These published proceedings and journals involve internationally with other researchers from around the world.

Book chapters:

- **K. Yamashita**, C-W. Ten, and L. Wang, "Dynamical Analysis of Cyber-Related Contingencies Initiated from Substations," under special edition of "Security for Cyber-Physical Systems: Vulnerability and Impact," edited by Hadis Karimipour, Pirathayini Srikantha, Hany Farag, and Jin Wei-Kocsis (the editors), pp. 223-246, Springer, Cham, 2020.

Article published in journals (related to this dissertation):

- **K. Yamashita**, C-W. Ten, Y. Rho, L. Wang, W. Wei, and A. Ginter, "Measuring Systemic Risk of Switching Attacks based on Cybersecurity Technologies in Substations," IEEE Transactions on Power Systems, Vol. 35, No. 6, pp. 4206-4219, Nov. 2020.

- C-W. Ten, **K. Yamashita**, Z. Yang, A. Vasilakos, and A. Ginter, "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems," IEEE Transactions on Smart Grid, Vol. 9, No. 5, pp. 4405 - 4425, Sep. 2018.

Article published in journals (non-related to dissertation with affiliation of Michigan Technological University):

- H. Satoh, **K. Yamashita**, K. Shirasaki, and Y. Kitauchi, "Root-mean Square Model of Three-Phase PhotovoltaicInverter for Unbalanced Fault," IEEE Open Access Journal of Power and Energy, accepted as publication on 9/17/2020.

- D. Zhao, M. Qian, J. Ma, **K. Yamashita**, "Photovoltaic generator model for power system dynamic studies," Solar Energy, Vol. 210, pp. 101-114, 2020.

- S. Su, Yong Hu, Luobin He, **K. Yamashita**, and Shidan Wang, "An Assessment

Procedure of Distribution Network Reliability Considering Photovoltaic Power Integration," IEEE Access, Vol. 7, pp. 60171-60185, May 2019.

Other article published in journals (non-related papers to dissertation):

- J. Ma, D. Zhao, L. Yao, M. Qian, **K. Yamashita**, and L. Zhu, "Analysis on application of a current-source based DFIG wind generator model," CSEE Journal of Power and Energy Systems, Vol. 4, No. 3, pp 352-361, Sep. 2018.

- L. Korunovic, J. V. Milanovic, S. Z. Djokic, **K Yamashita**, S. M. Villanueva, and S. Sterpu, "Recommended Parameter Values and Ranges of Most Frequently Used Static Load Models," IEEE Transactions on Power Systems, May 2018.

- **K. Yamashita**, H. Renner, S. M. Villanueva, G. Lammert, P. Aristidou, J. C. Martins, L. Zhu, L. D. P. Ospina, and T. V. Cutsem, "Industrial Recommendation of Modeling of Inverter Based Generators for Power System Dynamic Studies with Focus on Photovoltaic," IEEE Power and Energy Technology Systems Journal, Vol. 5, No. 1, pp. 1-10, March 2018.

- S. Su, Y. Hu, T. Yang, S. Wang, Z. Liu, X. Wei, M. Xia, Y. Ota, and **K. Yamashita**, "Research on an Electric Vehicle Owner-Friendly Charging Strategy Using Photovoltaic Generation at Office Sites in Major Chinese Cities," Energies, Vol

11, No. 2, Feb. 2018.

- S. Su, Y. Hu, S. Wang, W. Wang, Y. Ota, **K. Yamashita**, M. Xia, X. Nie, L. Chen, and X. Mao, "Reactive power compensation using electric vehicles considering drivers' reasons," IET Transactions on Generation, Transmission & Distribution, Jan. 2018.

- G. Lammert, **K. Yamashita**, L. D. Pabon Ospina, H. Renner, S. Martinez Villanueva, P. Pourbeik, F.-E. Ciausiu, and M. Braun, "Modelling and Dynamic Performance of Inverter Based Generation in Power System Studies: An International Questionnaire Survey," CIRED -Open Access Proceedings Journal, Vol. 1, 2017.

- G. Lammert, **K. Yamashita**, L. D. Pabon Ospina, H. Renner, S. Martinez Villanueva, P. Pourbeik, F.-E. Ciausiu, and M. Braun, "International Industry Practice on Modelling and Dynamic Performance of Inverter Based Generation in Power System Studies," CIGRE Science & Engineering, Vol. 8, June 2017.

- J. V. Milanovic, **K. Yamashita**, S. Marinez Villanueva, S. Ž. Djokic, L. M. Korunovic, "International Industry Practice on Power System Load Modeling," IEEE Trans. on Power Systems, Vol. 28, No. 3, pp. 3038-3046, 2013.

- **K. Yamashita**, J. Li, C.-C. Liu, P. Zhang, and M. Hofmann, "Learning to Recognize Vulnerable Patterns Due to Undesirable Zone-3 Relay Operations," IEEJ Transactions on Electrical and Electronic Engineering, Vol. 4, No. 3, 2009.

- **K. Yamashita**, Sung-Kwan Joo, J. Li, P. Zhang, C.-C. Liu, "Analysis, Control,

and Economic Impact Assessment of Major Blackout Events," European Transactions on Electrical Power, Vol. 8, No. 11, pp. 854-871, 2008.

- T. Matsumoto, Y. Kurosawa, M. Usui, **K. Yamashita**, and T. Tanaka, "Experience of Numerical Protective Relays Operating in an Environment With High-Frequency Switching Surge in Japan," IEEE Transactions on Power Delivery, Vol. 21, No. 1, pp. 88-93, 2006.

Article published in conference papers (non-related to dissertation with affiliation of Michigan Technological University):

- J. Shi, B. Foggo, X. Kong, Y. Cheng, N Yu, and **K. Yamashita**, "Online Event Detection in Synchrophasor Data with Graph Signal Processing," Proceedings of 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Virtual Conference, Nov. 11-13, 2020.

- J. Shi, N. Yu, E. Keogh, H. Chen, and **K. Yamashita**, "Discovering and Labeling Power System Events in Synchrophasor Data with Matrix Profile," Proceedings of 2019 IEEE Sustainable Power & Energy Conference, Beijing, China. Nov. 2019.

Chapter 2

Modeling of Steady-State Probabilities in Substations

2.1 Quantifying Metrics for Electronic Intrusion

2.1.1 Attacks Upon IP-based Substations

Attacks upon substation can be one of the growing concerns from the power system security point of view. Especially after the Ukraine substation attacks in 2015 and 2016 [112], many people around the world started to realize that the substation attack is no longer science fiction. Besides, such events made us aware that the cyber-physical

world and the real world are now seamless.

Power system security is one aspect of the power system reliability triggered by a system event such as system fault, *i.e.* lightning strokes, and disconnection of power equipment, *i.e.* generator tripping, and load shedding. Because the system event initiated almost all large blackouts, power system engineers have paid attention to the possible future threat that can violate the power system security, *i.e.* large blackouts. The dependence on electricity has increased, and uninterrupted electricity is vital for the current society. Such cyberattacks on substation can even threaten human life. Therefore, the substation attack is highly likely to be one of the future threats not only for the power companies but for the entire nation.

2.1.2 General Footprints to an IP-Based Substation

The hacking of the substation in Ukraine was initiated by hacking the control system in six substations in Ukraine. The hacking of the control system is attained via cracking the firewall and the password of the server in the substation. Then, our interest becomes the frequency or the probability of the substation attack with its impact (*i.e.* loss of electricity in the targeted grid). From the power system planner's point of view, not only the probability of the next blackout caused by the substation attack next year but also the averaged probability of the substation attack for a long

time becomes crucial. The latter is also known as the term, *steady-state probability* in the probability theory or stationery distribution in the stationery process.

2.1.3 Characterizing Intrusion Process

2.1.3.1 Markov Chain

The stationery distribution is often discussed in the Markov chain. To obtain a clearer picture, let's assume that substation attacks consist of three states, as shown in Fig. 2.1.

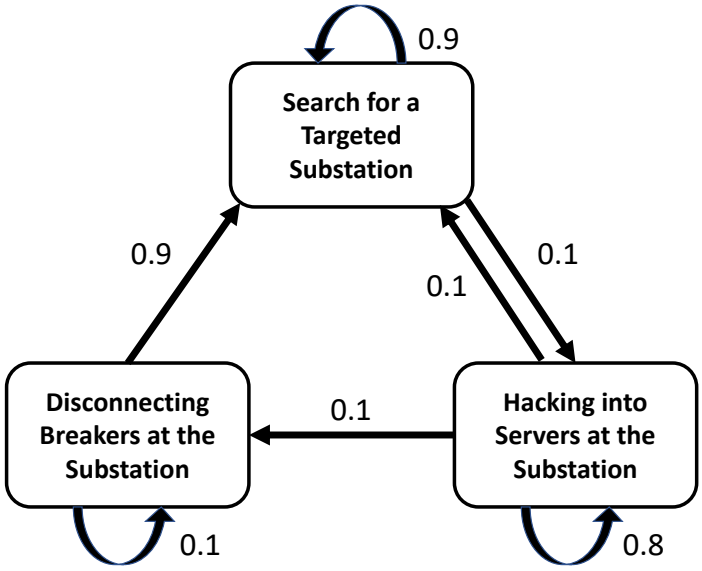


Figure 2.1: Example of attack transitions to substation network

In this example, the state space is represented as $S = \{S_1, S_2, S_3\}$ where,

S_1**:** Search for a Targeted Substation

S_2**:** Hacking into Servers at the Substation

S_3**:** Disconnecting Breakers at the Substation

When the state at time m is defined as $\{X_m\}$, the probability of this state, and the transition probability from one state to another are expressed as $P(X_m)$ and $P(X_{m+1}|X_m)$, respectively. In this example in Fig. 2.1, $P(X_{m+1} = S_2|X_m = S_1) = 0.1$ and $P(X_{m+1} = S_2|X_m = S_2) = 0.8$.

The Markov chain is defined as Equation (2.1) using a state at time m, $\{X_m\}$.

$$P(X_{m+1}|X_m, \ldots, X_1, X_0) = P(X_{m+1}) \tag{2.1}$$

The meaning of this equation can be summarized as two bullet points:

- X_{m+1} is determined by X_m only
- $X_{m-1}, X_{m-2}, X_{m-3}$... are nothing to do with X_{m+1}

In this example, it can be stated that disconnecting breakers is nothing to do with searching for the targeted substation but has much to do with cracking the server at

the substation only. This characteristics shown in Equation (2.1) is called Markov property. When the Markov chain and its relevant theorems are used, the Markov property for the created Markov chain model needs to be tested first. If the Markov property is not justified, the Markov chain model needs to be further updated, and the segmentalize the states, *i.e.* increasing the number of states is known as a general countermeasure. Therefore, the Markov chain can be utilized, especially when the action flow or procedure is clarified.

2.1.3.2 Stationery Distribution

The stationery distribution in the Markov chain is a set of state transition probabilities that is time-invariant after transiting from one state to another infinitely. Let's discuss the stationery distribution of the *discrete-time* Markov chain. It is noted that the Markov chain has two types: 1) discrete-time Markov chain 2) continuous-time Markov chain. When the discrete-time Markov chain is given as X_m, n-step ahead transition probability from the state i to the state j at the time, m is described as Equation (2.2).

$$p_{ij}(m,n) = P(X_{m+n} = j | X_m = i) \tag{2.2}$$

The n-step ahead transition probability matrix at the time, m is described as Equation (2.3).

$$\mathbf{P}(m,n) = p_{ij}(m,n) \tag{2.3}$$

where,

$$\mathbf{P}(m,0) = \mathbf{I} \tag{2.4}$$

If the transition probability matrix, P is time-invariant, the Markov chain is called a time-homogeneous Markov chain and is represented as Equation (2.5).

$$\forall m, n \geq 0, \mathbf{P}(m,n) = \mathbf{P}(0,n) = \mathbf{P}^{(n)} = (p_{ij}^{(n)}) \tag{2.5}$$

The stationary distribution of the time-homogeneous Markov chain, π is defined as Equation (2.6) using the transition probability matrix, P.

$$(\pi_1, \pi_2, ..., \pi_k)\mathbf{P} = (\pi_1, \pi_2, ..., \pi_k) \tag{2.6}$$

$$\pi_1 + \pi_2 + ... + \pi_k = 1 \tag{2.7}$$

To obtain a clear image, let's use the previous example in 2.1. The transition probability matrix, P is expressed as Equation (2.8). It can be realized that the summation of each row is always one. In other words, the summation of the probabilities from one state to another (including the same state) needs to be always one. This is an important property that the Markov chain owns.

$$\mathbf{P} = \begin{pmatrix} 0.9 & 0.1 & 0.0 \\ 0.1 & 0.8 & 0.1 \\ 0.9 & 0.0 & 0.1 \end{pmatrix} \tag{2.8}$$

Because a row vector, π needs to be satisfied with Equations (2.6) and (2.7), the simultaneous equation is created introducing $\pi = \{\pi_1, \pi_2, \pi_3\}$ as shown in Equation (2.9).

$$
\begin{aligned}
0.9\pi_1 + 0.1\pi_2 + 0.9\pi_3 &= \pi_1 \\
0.1\pi_1 + 0.8\pi_2 &= \pi_2 \\
0.1\pi_2 + 0.1\pi_3 &= \pi_3 \\
\pi_1 + \pi_2 + \pi_3 &= 1
\end{aligned} \tag{2.9}
$$

Then, the solution is derived as Equation (2.10). These probabilities represent the stationary distribution, *i.e.* steady-state probabilities. Then, it can be realized that the disconnection of breakers is rarely occurred because of the low probability, and most hackers must search for the targeted substation. Once we create the accurate Markov chain model, such state probability can be quantitatively clarified.

$$
(\pi_1, \pi_2, \pi_3) = \left(\frac{18}{28}, \frac{9}{28}, \frac{1}{28} \right) \tag{2.10}
$$

2.1.3.3 Limit Distribution

The limit distribution is defined as Equation (2.11).

$$\lim_{m\to\infty} \pi_m = \lim_{m\to\infty} \pi_0 P^m \tag{2.11}$$

It should be noted that the limit distribution is not always the same as the stationary distribution. Only if the stationery distribution is not *aperiodic*, this is identical to the limit distribution. A typical periodic stationary distribution is shown below.

The transition probability matrix, P is given in Equation (2.12).

$$\mathbf{P} = \begin{pmatrix} 0.0 & 1.0 & 0.0 \\ 0.3 & 0.0 & 0.7 \\ 0.0 & 1.0 & 0.0 \end{pmatrix} \tag{2.12}$$

Then P^2, P^3, and P^4 are derived as Equations (2.13)-(2.15).

$$\mathbf{P^2} = \begin{pmatrix} 0.3 & 0.0 & 0.7 \\ 0.0 & 1.0 & 0.0 \\ 0.3 & 0.0 & 0.7 \end{pmatrix} \tag{2.13}$$

$$\mathbf{P^3} = \begin{pmatrix} 0.0 & 1.0 & 0.0 \\ 0.3 & 0.0 & 0.7 \\ 0.0 & 1.0 & 0.0 \end{pmatrix} \tag{2.14}$$

$$\mathbf{P^4} = \begin{pmatrix} 0.3 & 0.0 & 0.7 \\ 0.0 & 1.0 & 0.0 \\ 0.3 & 0.0 & 0.7 \end{pmatrix} \tag{2.15}$$

Therefore, examining the periodicity of the stationery distribution is important to conclude if the steady-state probability can be obtained. In the example in Fig. 2.1, the stationery distribution shown in Equation (2.10) is not aperiodic, *i.e.* the stationery distribution represents the steady-state probabilities.

2.1.3.4 Continuous-Time Markov Chain

Markov chain is represented using the continuous-time Markov process as well as the discrete-time Markov process. All the previous discussions are based on the

discrete-time Markov process, and the difference between the two Markov chains are summarized below:

- Discrete-time Markov chain: The transition probability from the state i at the time m, to the state j at the time $m+1$ depends on only the state, $X_m = i$ (see Fig. 2.2).
- Continuous-time Markov chain: The transition probability from the state i at the time s, to the state j at the time $s+t$ depends on the time difference, t (see Fig. 2.3).

As shown in the above bullet points, the continuous-time Markov chain's unique characteristics are that the time to transit from one state to another is variable, as shown in Fig. 2.3. Strictly speaking, the sojourn time at one state can vary, while the transition is performed instantaneously (*i.e.* the transition time is zero). In the example in Fig. 2.1, the time to disconnecting breakers from successfully hacking servers at the targeted substation can vary depending on how long the hackers struggles to figure out the way of how to disconnect breakers at the targeted substation.

In the continuous-time Markov chain, the sojourn time at a state spreads according to

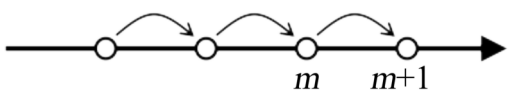


Figure 2.2: Discrete-Time Markov process

Figure 2.3: Continuous-Time Markov process

an exponential distribution. Suppose the sojourn time at a state spreads according to other distributions such as alpha-, beta-, chi-, and gamma. In that case, distributions, the Markov property's stochastic process, is more generalized and called continuous-time *Semi*-Markov chain.

2.2 Irregular Event Abstraction Using Petri-Net Models

2.2.1 Properties of Petri Net

A substation attack occurs through several significant steps. 1) cracking firewall, 2) cracking password, 3) hacking into control server, 4) isolate electrical equipment at the substation such as connected transmissions and transformers and buses via disruptive switching attacks. Those steps may be treated as a state, and the sequence of steps may be represented as an Automaton that comprises "state" and "transition" (Fig. 2.4). Petri net enhances the representation capability and is one of the graphs and

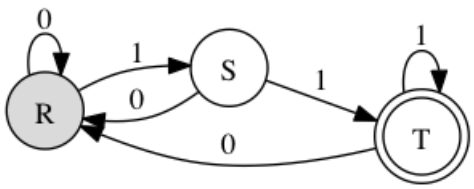


Figure 2.4: Automaton

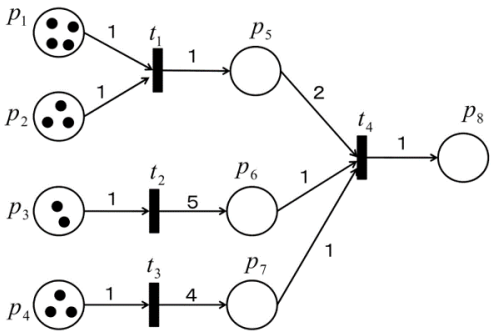


Figure 2.5: Petri net

a place and transition net with input and output arcs. One of the most significant advantages of using the Petri net is that the notion of time can be added (Fig. 2.5).

The fundamental mechanism is shown in Fig. 2.6. Circles denote a place in a Petri net model. In this example in Fig. 2.6, one token is shown in a place. The token on the left-hand side is called the initial token that represents an initial condition. Between the two places, one transition is expressed as an open bar. When the transition is ready to activate, it is said that the transition is fired. Then, the token in the input place is jumped to the output place. It is noted that the transition time is ignored in the Petri net.

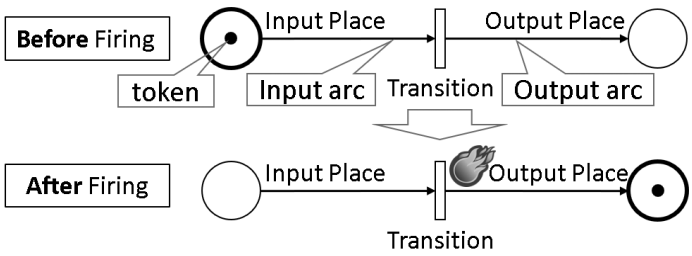


Figure 2.6: Transition mechanism of Petri net

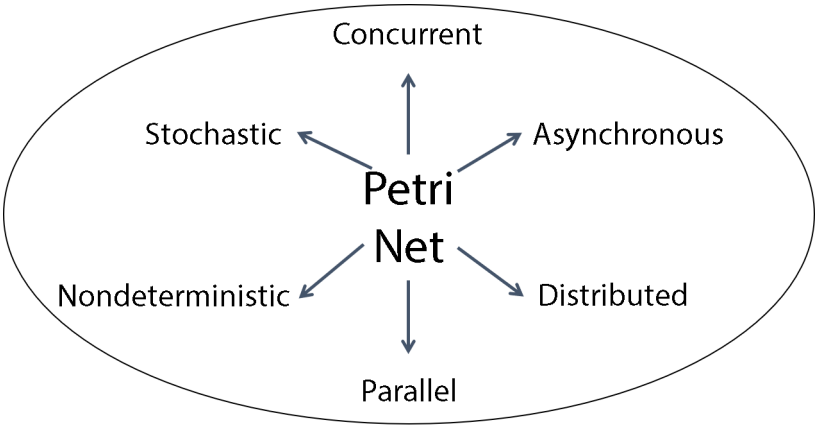


Figure 2.7: Representation capability of Petri net

Petri net is suited for expressing the concurrent, asynchronous, stochastic, nondeterministic, and distributed systems. So, the Petri net enables us to model a wide variety of systems with those operations (Fig. 2.7).

Another significant aspect is that the Petri net has three faces. The first one is a graphic tool. Other competitors can be a flowchart or a block diagram. The second one is the simulation tool. We can simulate concurrent and dynamic events using Petri net. The third one is mathematical methodology. We can create the state equation or algebraic equation for the targeted system via the Petri net model. Although the Petri net model was proposed in the 1960s, this is still the only tool with those three

faces.

2.2.2 Modeling the Extension

Petri net is a graph-based modeling tool that has been extensively researched. Over time, the Petri net has been evolving that introduces different types of transitions. Figures 2.8 and 2.9 show various types of Petri net and their evolving history, individually. Timed Petri net introduces a notion of time, *i.e.* a fixed timed transition. Then, the stochastic Petri net extended the functionality of the timed transition introducing the exponentially distributed timed transition. This enables us to map to the continuous-time Markov chain. Generalized stochastic Petri net adds a new type of transition, named immediate transition, together with the exponentially distributed timed transition. Enhanced stochastic Petri net allows us to use other distribution functions for the timed transition.

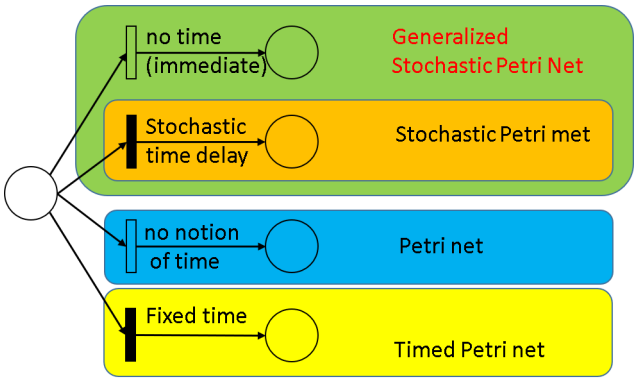


Figure 2.8: Various Petri net

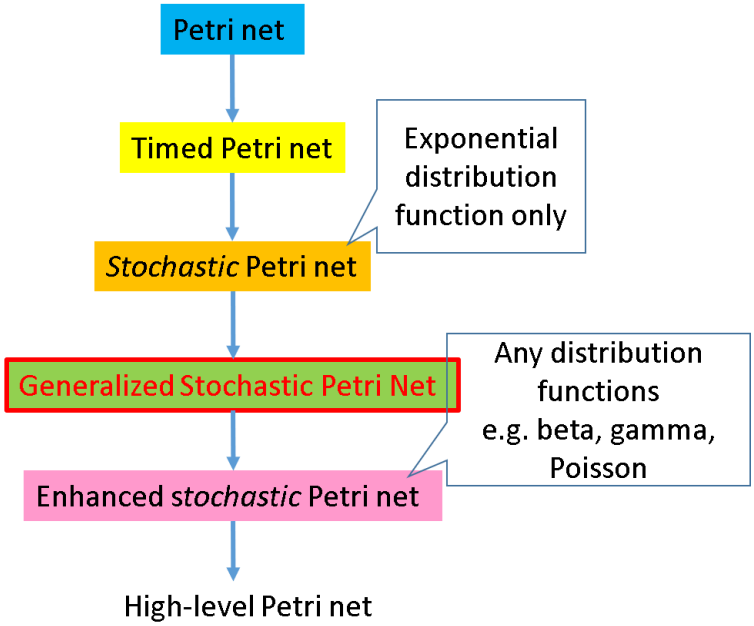


Figure 2.9: Enhanced Petri net

Due to the space limitation, the generalized stochastic Petri net (GSPN) is focused for modeling substation attacks.

2.2.3 Generalization of Stochastic Events

2.2.3.1 Definition for Simplified Firewall Model

Figure 2.10 shows an example of GSPN that represents a simplified firewall model. The GSPN is represented as the GSPN of P, T_1, T_2, A, W, and M_0. The meaning of those variables are:

- P: set of places
- T_1: Branching probability for immediate transition
- T_2: Transition rate for timed transition
- A: set of arcs
- W: set of weights of arcs
- M_0: initial marking

Solid bar in Fig. 2.10 denotes the immediate transition and the open bar denotes the timed transition. In this example, the tuple of describing the GSPN is as follows:

$$\begin{aligned} \text{GSPN} &= \{P, T_1, T_2, A, W, M_0\} \\ P &= \{p_1, p_2, p_3, p_4\} \\ T_1 &= \{t_1, t_2\} \\ T_2 &= \{\tau_3, \tau_4, \tau_5\} \\ W &= \{w_1, w_2, w_3, w_4, w_5\}, \\ M_0 &= (1, 0, 0, 0) \end{aligned}$$

where p_1 denotes the initiation of the firewall rule cracking, and p_2 denotes the successful cracking of firewall rules. Places, p_3 denotes the failure to crack firewall rules.

The place, p_4 denotes reaching to password input screen of the server. Variables, t_1 denotes the transition *probabilities* of the successful cracking of firewall rules. Variables, t_2 denotes the transition *probabilities* of the failure to crack firewall rules. Variables, τ_3 denotes the transition *rate* of responding to attackers opening a port. Variables, τ_4 denote the transition *rates* of responding to attackers indicating the password input screen. Variables, τ_5 denote the transition *rates* of responding to attackers denying opening any ports.

In this example, the GSPN consists of a set of 4 places, 2 immediate transitions probabilities, 3 timed transitions, 10 arcs, and 10 weights of arcs. When marking is defined as the number of tokens at p_1, p_2, p_3, and p_4, the initial marking, M_0 is expressed as $M_0 = [1, 0, 0, 0]$.

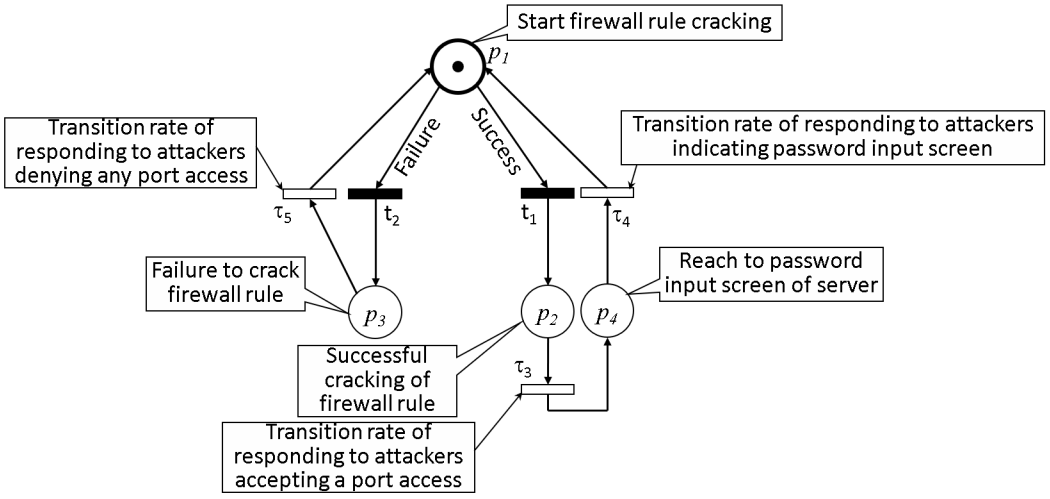


Figure 2.10: Example of GSPN

2.2.3.2 Reachability Graph Mapping to Markov Chain

To map the GSPN to the Markov chain, markings' transition is more focused instead of the transition of places. It is realized that GSPN transits from M_0 to M_1 or M_2 by firing the immediate transitions t_1 or t_2. Because the immediate transition is used, M_0 is called *vanishing marking*, *i.e.* no waiting time at a state (and no transition time from one place to another). The GSPN transits from M_2 to M_0 by the timed transition of τ_5. The GSPN also transits from M_1 to M_3 or from M_3 to M_4 by the timed transitions, τ_3 and τ_4, respectively. When only timed transitions are used to transit from the current marking to other markings, this marking is called tangible marking. In this example, M_1, M_2, and M_3 are the tangible marking. Hereafter, the superscript, V and T are added to vanishing markings and tangible markings, individually.

The graph that consists of those markings and their arcs is called a reachability graph (Fig. 2.11). In the reachability graph, the term, *weight*, is newly introduced because the transition probability and the transition rate are not differentiated in the reachability graph. Therefore, the values of the immediate transitions and the timed transitions are used as they are, as the weight of the reachability graph.

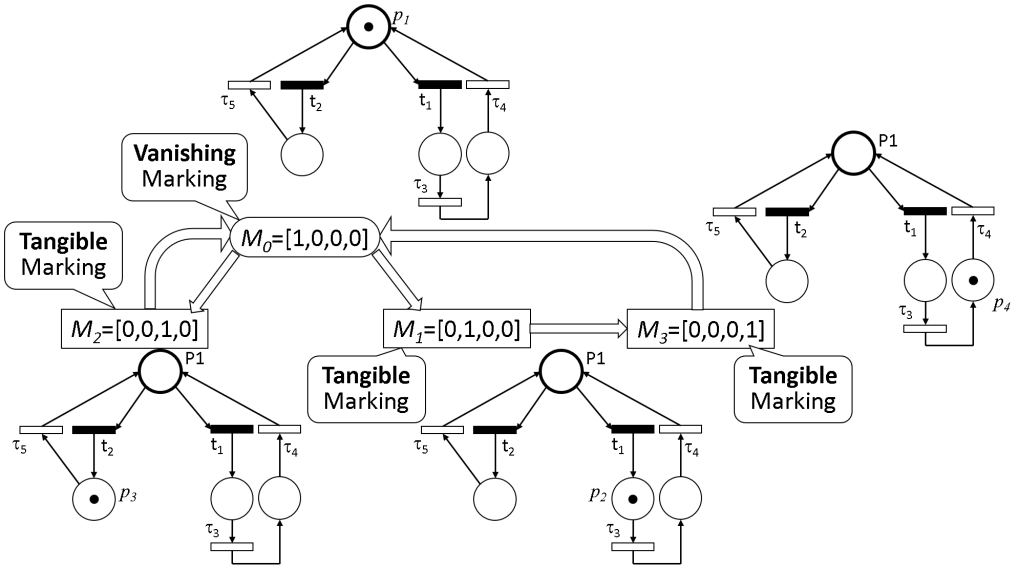


Figure 2.11: Reachability graph of firewall Petri net

2.2.3.3 Transition Probability Matrix for Semi-Markov Chain and Continuous-Time Markov Chain

Once a reachability graph is generated, a transition probability matrix is created in the followings.

- Vanishing marking: weights, *i.e.* transition probabilities are input as they are.
- Tangible marking: weights needs to be normalized at each row of the transition probability matrix.

Let's assume imputed values for the immediate transition and the timed transition show below (Fig. 2.12):

- $T_1 = \{t_1 = 0.001,\ t_2 = 0.999\}$
- $T_2 = \{\tau_3 = 10^{-6},\ \tau_4 = 10^{-6},\ \tau_5 = 0.5 \times 10^{-6}\}$

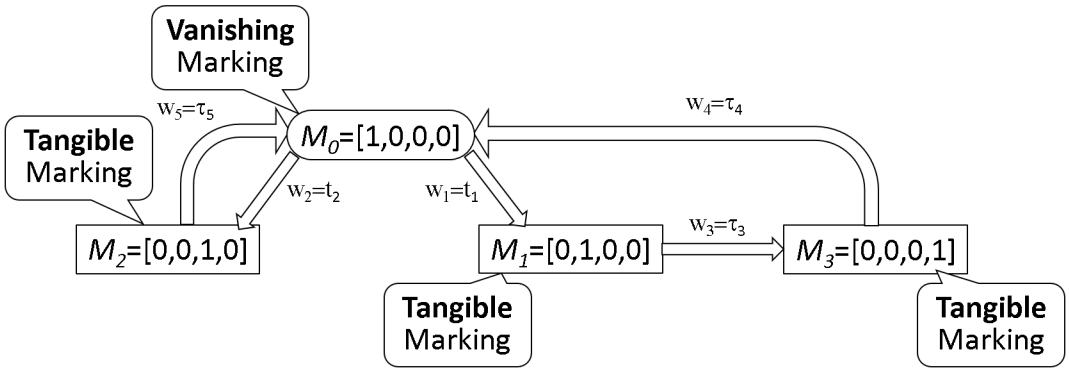


Figure 2.12: Extended reachability graph

In this example, the rate probability matrix, U that consists of the transition rate from each tangible marking to each vanishing or tangible marking, is expressed as Equation (2.16).

$$\mathbf{U^T} = \left(U^{TV}|U^{TT}\right) = \begin{array}{c} \\ M_1^T \\ M_2^T \\ M_3^T \end{array} \begin{array}{c} \begin{array}{cccc} M_0^V & & M_1^T & M_2^T & M_3^T \end{array} \\ \begin{pmatrix} 0 & |\,0 & 0 & 10^{-6} \\ 10^6 & |\,0 & 0 & 0 \\ 0.5 \times 10^{-6} & |\,0 & 0 & 0 \end{pmatrix} \end{array} \tag{2.16}$$

Here, the probability matrix, P consists of the transition probability from each vanishing marking to each tangible marking or vanishing marking, other than the normalized

rate transition matrix. The sub-matrix of P that consists of the transition probability from each vanishing marking to each tangible marking or vanishing marking is expressed as Equation (2.17).

$$\mathbf{P^V} = \begin{array}{c} \\ M_0^V \end{array} \begin{array}{c} \begin{array}{cccc} M_0^V & M_1^T & M_2^T & M_3^T \end{array} \\ \begin{pmatrix} 0 & 0.001 & 0.999 & 0 \end{pmatrix} \end{array} \tag{2.17}$$

The probability matrix seems to be calculated combining matrices, P^V and U^T as shown in Equation (2.18). However, the Markov property requires a condition that the summation of each row in the transition probability matrix is always 1.

$$\begin{pmatrix} P^V \\ U^T \end{pmatrix} = \begin{array}{c} \\ M_0 \\ M_1 \\ M_2 \\ M_3 \end{array} \begin{array}{c} \begin{array}{cccc} M_0^V & M_1^T & M_2^T & M_3^T \end{array} \\ \begin{pmatrix} 0 & 0.001 & 0.999 & 0 \\ 0 & 0 & 0 & 10^{-6} \\ 10^{-6} & 0 & 0 & 0 \\ 0.5 \times 10^{-6} & 0 & 0 & 0 \end{pmatrix} \end{array} \tag{2.18}$$

The probability matrix seems to be calculated combining matrices, P^V, and U^T, as shown in Equation (2.18). However, the Markov property requires a condition that the summation of each row in the transition probability matrix is always 1.

$$\mathbf{P^T} = \begin{array}{c} \\ M_1^T \\ M_2^T \\ M_3^T \end{array} \begin{array}{c} \begin{array}{cccc} M_0^V & M_1^T & M_2^T & M_3^T \end{array} \\ \left(\begin{array}{c|ccc} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{array}\right) \end{array} \tag{2.19}$$

Thus, the transition probability matrix, P can be expressed as Equation (2.20).

$$\mathbf{P} = \begin{pmatrix} P^V \\ P^T \end{pmatrix} = \begin{array}{c} \\ M_0 \\ M_1 \\ M_2 \\ M_3 \end{array} \begin{array}{c} \begin{array}{cccc} M_0^V & M_1^T & M_2^T & M_3^T \end{array} \\ \begin{pmatrix} 0 & 0.001 & 0.999 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array} \tag{2.20}$$

The tangible marking has a certain sojourn time at the corresponding marking, while the vanishing marking has no sojourn time at the corresponding marking. Because of no sojourn time for vanishing markings, the transition probability becomes zero, and vanishing markings can be eliminated from the transition probability matrix shown in Equation (2.20). The reduced transition probability matrix, P' is derived from Equation (2.21).

$$\mathbf{P}' = P^{TT} + P^{TV}\left(I - P^{VV}\right)P^{VT}$$

where

$$\mathbf{P} \equiv \begin{pmatrix} P^{VV} & P^{VT} \\ P^{TV} & P^{TT} \end{pmatrix} \tag{2.21}$$

In this example, the matrix dimension is reduced from four to three, as shown in Equation (2.22). Because only exponentially distributed timed transitions remain in the reduced transition probability matrix, it becomes the probability transition matrix used for the Markov chain.

$$\mathbf{P}' \equiv \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} (.001\ .999\ 0) = \begin{pmatrix} 0 & 0 & 1 \\ .001 & .999 & 0 \\ .001 & .999 & 0 \end{pmatrix} \tag{2.22}$$

This reduction of the transition matrix, removing the vanishing markings, contributes to computational efficiency by formulating this problem with the continuous-time Markov chain instead of the semi-Markov chain.

2.2.3.4 Steady-State Probability for Continuous-Time Markov Chain

It can be recognized that the derived transition probability matrix, P' has the same form in Equation (2.8), which means the steady-state probability can be calculated using the same procedure that was explained in Clause 2.1.3. Substituting Equation (2.22) into Equation (2.6) and utilizing Equation (2.7), the steady-state probability is derived as Equation (2.23).

$$
\begin{aligned}
0.001\tilde{\pi}_2 + 0.001\tilde{\pi}_3 &= \tilde{\pi}_1 \\
0.999\tilde{\pi}_2 + 0.999\tilde{\pi}_3 &= \tilde{\pi}_2 \\
\tilde{\pi}_1 &= \tilde{\pi}_3 \\
\tilde{\pi}_1 + \tilde{\pi}_2 + \tilde{\pi}_3 &= 1
\end{aligned}
$$

$$
\therefore (\tilde{\pi}_1, \tilde{\pi}_2, \tilde{\pi}_3) = (0.001, 0.998, 0.001) \tag{2.23}
$$

It should be noted that the probabilities in Equation (2.23) is derived mapping GSPN

to continuous-time Markov chain, *i.e.* using the *normalized* P^T. Therefore, the derived steady-state probabilities need to be mapped from the continuous-time Markov chain to GSPN.

2.2.3.5 Steady-state Probability for GSPN

The steady-state probability is calculated from both the steady-state distribution, $\tilde{\pi}_i|_{i=1,2,...}$ and the corresponding sojourn times, $h_i|_{i=1,2,...}$. The expected sojourn time (also known as holding time) h_i at a marking state i can be derived from the transition *rate* matrix U^T. The sojourn time, h_i is derived from Equation (2.24).

$$h_i = \begin{cases} \dfrac{1}{\sum\limits_{j \in V \cup T} U^T_{i,j}}, & \text{if } i \in \text{Tangible Markings} \\ 0, & \text{if } i \in \text{Vanishing Markings.} \end{cases} \tag{2.24}$$

In this example in Fig. (2.10), the sojourn times, h_1, h_2, and h_3 are calculated as shown in Equation (2.25).

$$
\begin{aligned}
h_1 &= \frac{1}{w_3} = \frac{1}{\tau_3} = \frac{1}{10^{-6}} : \ M_1^T -> M_3^T \\
h_2 &= \frac{1}{w_5} = \frac{1}{\tau_5} = \frac{1}{0.5 \times 10^{-6}} : \ M_2^T -> M_0^V \\
h_3 &= \frac{1}{w_4} = \frac{1}{\tau_4} = \frac{1}{10^{-6}} : \ M_3^T -> M_0^V
\end{aligned}
\tag{2.25}
$$

Once h_i is obtained, the steady-state probability is generally calculated from Equation (2.26). Then, the steady-state probability for the GSPN in Fig. 2.10 is calculated as Equation (2.27).

$$
\pi_{i|i=1,2,\ldots} = \frac{\tilde{\pi}_i h_i}{\sum\limits_{j \in V \cup T} \tilde{\pi}_j h_j} = \frac{\tilde{\pi}_i h_i}{\sum\limits_{j \in T} \tilde{\pi}_j h_j}
\tag{2.26}
$$

$$
\begin{aligned}
\pi_1 &= \frac{\frac{\tilde{\pi}_1}{10^{-6}}}{\frac{\tilde{\pi}_1}{10^{-6}} + \frac{\tilde{\pi}_2}{0.5 \times 10^{-6}} + \frac{\tilde{\pi}_3}{10^{-6}}} = 0.0005 \\
\pi_2 &= \frac{\frac{\tilde{\pi}_2}{0.5 \times 10^{-6}}}{\frac{\tilde{\pi}_1}{10^{-6}} + \frac{\tilde{\pi}_2}{0.5 \times 10^{-6}} + \frac{\tilde{\pi}_3}{10^{-6}}} = 0.999 \\
\pi_3 &= \frac{\frac{\tilde{\pi}_3}{10^{-6}}}{\frac{\tilde{\pi}_1}{10^{-6}} + \frac{\tilde{\pi}_2}{0.5 \times 10^{-6}} + \frac{\tilde{\pi}_3}{10^{-6}}} = 0.0005
\end{aligned}
\tag{2.27}
$$

Let's discuss the meaning of the steady-state probabilities, $\pi_{i|i=1,2,3}$ using this example in Fig. 2.10. Each π corresponds to the probability of each marking state. The marking state corresponds to each state (or the combination of states in the case of multiple tokens). As shown in Fig. 2.12, marking states, M_1, M_2, and M_3 corresponds to p_2, p_3, and p_4. As already mentioned, there is zero probability for the marking state, M_0 because this state is transited to either M_1 or M_2 immediately once the current state becomes M_0. Therefore, M_0 is not discussed as the steady-state probability.

As shown in Fig. (2.10) and Equation (2.27), the following probabilities are clarified.

- $M_1(=p_2)$: 0.1% of hackers successfully cracked firewall rules. Those hackers are waiting for incoming password input screen of servers in order to login to them.
- $M_3(=p_4)$: 0.1% of hackers are able to attempt the password cracking using the password input screen of servers in the targeted substation.
- $M_2(=p_3)$: 99.98% of hackers are struggling to cracking the firewall rule because they fail to crack them.

Thus, once the steady-state probabilities are calculated, the hackers' status can be clarified from a stochastic perspective. It should be emphasized that the steady-state probabilities show the probability after the elapse of an infinitely long period of time. As mentioned earlier, this type of indicator can be vital, especially when the countermeasure for substation attack needs to be designed in the industry.

2.2.3.6 Review of Procedure of How to Calculate Steady-state Probability of GSPN

The entire procedure of how to derive the steady-state probability for GSPN is summarized in Fig. 2.13. As shown in Fig. 2.13, the Markov property is effectively utilized while the steady-state probability is calculated. Based on the extended reachability graph of the GSPN, the Semi-Markov chain is created first. After eliminating vanishing markings, *i.e.* immediate transitions with the normalization for the timed

transition, the continuous-time Markov chain is created. Thus, the steady-state probabilities are calculated under the continuous-time Markov chain. An inverse normalizing technique is applied to derive the steady-state probabilities of the GSPN. There are many available non-commercial tools and commercially available tools to calculate the steady-state probability of the GSPN. Therefore, once a GSPN is created, the steady-state probability is automatically calculated. Such tools also enable us to use different distributions other than the exponential distribution for the timed transition. Besides, they can even analyze how the probabilities are converged to the steady-state probabilities.

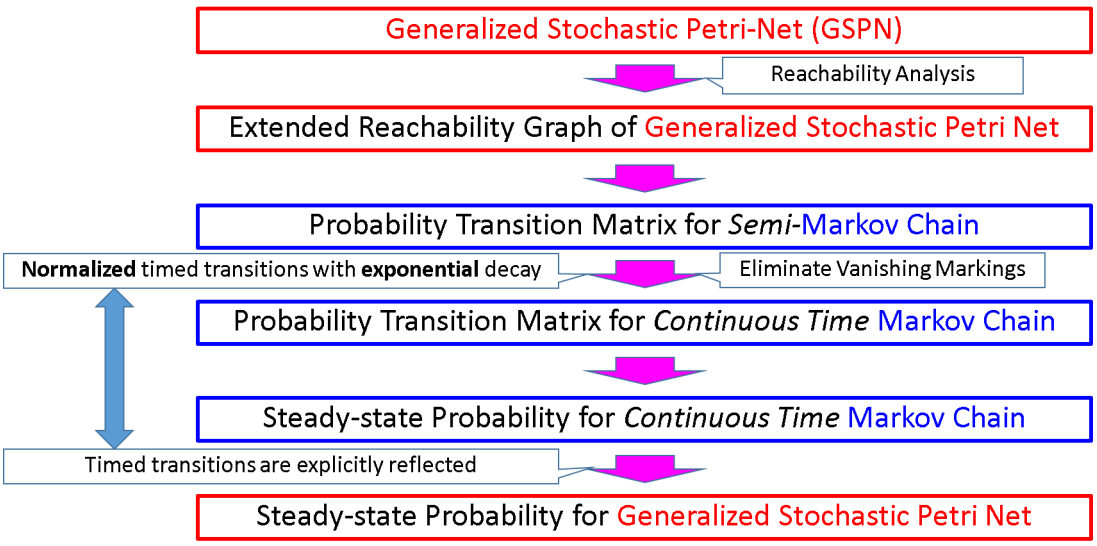


Figure 2.13: Procedure for steady-state probability of GSPN

Table 2.1
Statistical measure for places and transitions in GSPN

	Probability	Average
Place	Probability of being in a subset of markings $\Pr[B] = \sum_{M_i \in B} \pi_i$ $B \subseteq R(PN)$ *R(PN)* denotes reachability set of Petri Net	Mean Number of Tokens $E[m_i] = \sum_{n=1}^{k} \left(nP[B(p_i, n)] \right)$ $B(p_i, n) = \{ M \in R(PN) \mid M(p_i) = n \}$
Transition	Probability of firing transition $r_j = \sum_{M_i \in EN_j} \pi_i \frac{\tau_j}{-\tau_{jj}}$ τ_{jj} denotes sum of transition rates ***out of*** M_i	Throughput at a transition $E[d_i] = \sum_{M_i \in EN_j} \pi_i \tau_j$ *EN* denotes set of enabled transitions

2.2.3.7 Role of Tokens in GSPN and indicators obtained from GSPN

Once the steady-state probabilities for GSPN are obtained, the useful indicators shown in Table 2.1 are also obtained. If the initial token number is 1, the second column is the same as the third column. The indicator, *Throughput* provides the averaged number of tokens that move from one place to another. To clarify the steady-state probability of the substation attack, the place probability would be the most important indicator. Probability of B equals a summation of the expression π_i for M_i that belongs to B. B is a subset of the reachability of the Petri net.

2.3 Cyber-Net Examples Inferring Substation Anomalies

Although the risk of cybersecurity has been studied as a potential data breach, mainly in security businesses [113], their primary interests are to estimate the number of attacks shortly. A recent paper proposes a timed Petri net to estimate the steady-state probability of attacks on special protection scheme (SPS) [114]. Modeling the risk of intrusion and its processes based on security technologies is highly desirable. Technologies of deployed cyberinfrastructure and its associated anomalous events can be modeled in generalized stochastic Petri net (GSPN). The cyber-net defined in this Chapter is the construction of (bipartite) directed graph based on specific security technology, which can model the inter-dependencies of cyber components within a network. In this section, three fundamental models are introduced: (1) firewall model on control servers in substations, (2) password model on control servers (*i.e.* SCADA) in substations, (3) extended password model on intelligent electric device (IED), *i.e.* advanced protective relays in substations. Those three models are assembled to represent the cyber-net with new technologies shown in Fig. 1.2.

It is noted that weights, *i.e.*, transition probabilities and rates in Sub-section 2.3 are imputed with values within reasonable ranges.

2.3.1 Firewall Model

The example firewall model is enhanced based on the original establishment [25]. The tuple of describing the cyber-net model quantitatively and qualitatively is as follows:

$$
\begin{aligned}
\text{GSPN} &= \{P, T_1, T_2, A, W, M_0\} \\
P &= \{p_{\text{begin}}, p_{\text{rule1},\alpha}, p_{\text{rule1},\beta}, p_{\text{rule2},\alpha}, p_{\text{rule2},\beta}, p_{\text{rule3},\alpha}, p_{\text{rule3},\beta}, p_{\text{pass}}\} \\
T_1 &= \{t_{1,a}, t_{1,b}, t_{2,a}, t_{2,b}, t_{3,a}, t_{3,b}\} \\
T_2 &= \{\tau_{\text{rate},1}, \tau_{\text{rate},2}, \tau_{\text{rate},3}, \tau_{r,4}, \tau_{r,5}\} \\
M_0 &= (1, 0, 0, 0, 0, 0, 0, 0) \\
W &= \{w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8, w_9, w_{10}, w_{11}\},
\end{aligned}
$$

where

- The place, p_{begin} denotes the initiation of the firewall rule cracking.
- The places, $p_{\text{rule1},\alpha}$, $p_{\text{rule2},\alpha}$, and $p_{\text{rule3},\alpha}$ denote the successful cracking of firewall rules 1, 2, and 3, respectively.
- Places, $p_{\text{rule1},\beta}$, $p_{\text{rule2},\beta}$, and $p_{\text{rule3},\beta}$ denote the failure to crack firewall rules 1, 2, and 3, respectively.

- The place, p_{pass} denotes reaching to password input screen of the server.

- Variables, $t_{1,a}$, $t_{2,a}$, and $t_{3,a}$ denote the transition *probabilities* of the successful cracking of firewall rules 1, 2, and 3.

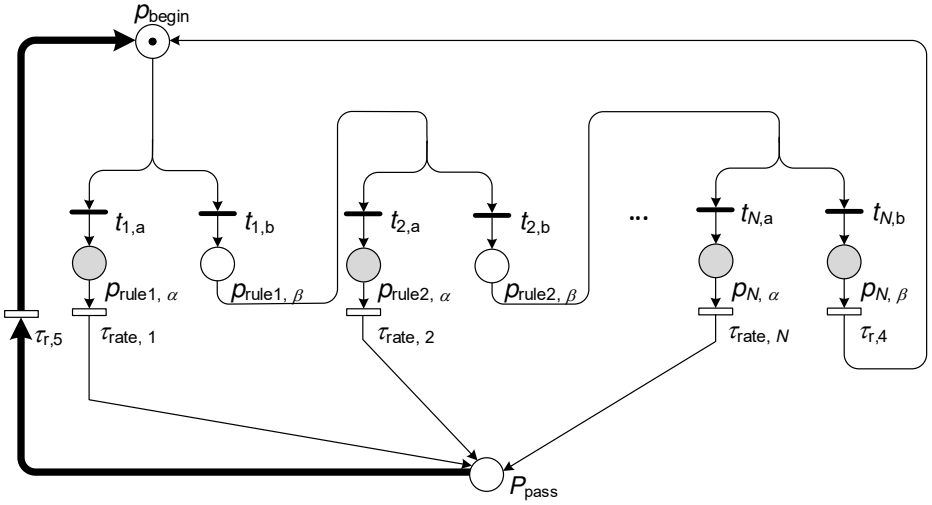
- Variables, $t_{1,b}$, $t_{2,b}$, and $t_{3,b}$ denote the transition *probabilities* of the failure to crack firewall rules 1, 2, and 3.

  Variables, $\tau_{\text{rate},1}$, $\tau_{\text{rate},2}$, and $\tau_{\text{rate},3}$ denote the transition *rate* of responding to attackers opening a port.

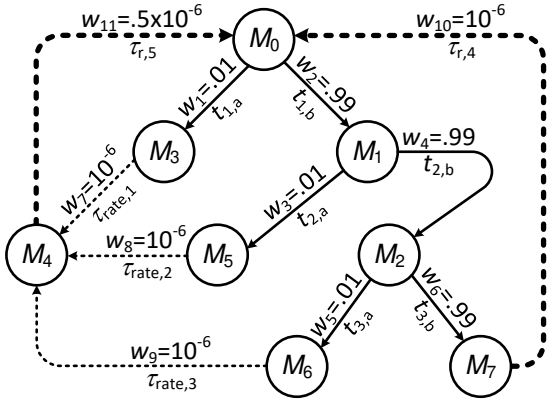
- Variables, $\tau_{r,4}$ and $\tau_{r,5}$ denote the transition *rates* of responding to attackers denying attackers of opening any ports and to attackers with status of password input, respectively.

The password cracking shows only two possibilities, *i.e.*, the successful login, or the login failure. Those probabilities are modeled as the immediate transition, and the sum of the two probabilities is one. On the other hand, the server's response time is not immediate, and such time delay is modeled as the timed transition. Therefore, the GSPN is applied to this model and the rest of the proposed models.

The reachability graph in Fig. 2.14 is an extended semi-Markovian Process because the sojourn time in each state is restricted to be either zero or exponentially distributed.



(a) Petri net model



	p_{begin}	$p_{rule1,\alpha}$	$p_{rule1,\beta}$	$p_{rule2,\alpha}$	$p_{rule2,\beta}$	$p_{rule3,\alpha}$	$p_{rule3,\beta}$	p_{pass}
M_0=[	1	0	0	0	0	0	0	0]
M_1=[	0	0	1	0	0	0	0	0]
M_2=[	0	0	0	0	1	0	0	0]
M_3=[	0	1	0	0	0	0	0	0]
M_4=[	0	0	0	0	0	0	0	1]
M_5=[	0	0	0	1	0	0	0	0]
M_6=[	0	0	0	0	0	1	0	0]
M_7=[	0	0	0	0	0	0	1	0]

(b) Reachability graph

Figure 2.14: Modified firewall model [21]

Define

$$
U^T = \begin{array}{c} \\ M_3^T \\ M_4^T \\ M_5^T \\ M_6^T \\ M_7^T \end{array}
\begin{array}{c}
\begin{array}{cccccccc} M_0^V & M_1^V & M_2^V & M_3^T & M_4^T & M_5^T & M_6^T & M_7^T \end{array} \\
\left(\begin{array}{c|ccccccc}
0 & 0 & 0 & 0 & 10^{-6} & 0 & 0 & 0 \\
5\times 10^{-7} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 10^{-6} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 10^{-6} & 0 & 0 & 0 \\
10^{-6} & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right)
\end{array}
$$

$$
= \left(\begin{array}{c|c} U^{TV} & U^{TT} \end{array} \right),
$$

the matrix describing the transition *rate* from each tangible marking to each vanishing or to tangible marking. The transition *probability* matrix, $\mathbf{P}$ can be represented as:

$$
\mathbf{P} = \left(\begin{array}{ccc|ccccc}
0 & .99 & 0 & .01 & 0 & 0 & 0 & 0 \\
0 & 0 & .99 & 0 & 0 & .01 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & .01 & .99 \\
\hline
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right)_{(8\times 8)}
$$

$$
= \left(\begin{array}{c} P^V \\ \hline P^T \end{array} \right) = \left(\begin{array}{c|c} P^{VV} & P^{VT} \\ \hline P^{TV} & P^{TT} \end{array} \right), \tag{2.28}
$$

where $P^V = (P^{VV} |\ P^{VT})$ denotes a matrix describing the transition probability from each vanishing marking to each vanishing or tangible marking, while $P^T = (P^{TV} |\ P^{TT})$ denotes a matrix describing the transition probability from each tangible marking to each vanishing or tangible marking. P^T is calculated from U^T normalizing the sum of each row to one.

In this firewall model, the rates corresponding to each timed transition can be written as a row vector

$$\begin{aligned} \boldsymbol{h} &= \left[0, 0, 0, \frac{1}{\tau_{\text{rate},1}}, \frac{1}{\tau_{r,5}}, \frac{1}{\tau_{\text{rate},2}}, \frac{1}{\tau_{\text{rate},3}}, \frac{1}{\tau_{r,4}}\right] \\ &= [0.0, 0.0, 0.0, 1.0, 2.0, 1.0, 1.0, 1.0] \times 10^6. \end{aligned} \tag{2.29}$$

Since $h_1 = h_2 = h_3 = 0$, the transition *probability* matrix, $\mathbf{P}$ may be reduced to a 5×5 matrix, $\mathbf{P}'$ using

$$\mathbf{P}' = P^{TT} + P^{TV}(I - P^{VV})^{-1}P^{VT}, \tag{2.30}$$

and thus

$$\mathbf{P}' = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ .01 & 0 & .0099 & .009801 & .9703 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ .01 & 0 & .0099 & .009801 & .9703 \end{pmatrix}_{(5\times 5)} . \tag{2.31}$$

The steady-state distribution, $\tilde{\pi}$ of the continuous time Markov chain is expressed as

$$\tilde{\pi}\mathbf{P}' = \tilde{\pi}; \sum_{M_j \in T} \tilde{\pi}_j = 1. \tag{2.32}$$

The steady-state distribution, $\tilde{\pi}$, for the tangible markings is derived as

$$\tilde{\pi} = [.009712, .02884, .009614, .009518, .94231]. \tag{2.33}$$

The steady-state probability $\pi_{j|j=1,\cdots,8}$ is calculated from both the steady-state distribution, $\tilde{\pi}_j$ and the corresponding holding times, h_j. For any j in tangible markings,

the steady-state probability is

$$\begin{aligned}\pi_{j|j=1,2,\cdots 8} &= \frac{\tilde{\pi}_j h_j}{\sum_{k\in V\cup T}\tilde{\pi}_k h_k} = \frac{\tilde{\pi}_j h_j}{\sum_{k\in T}\tilde{\pi}_k h_k} \\ &= \frac{\tilde{\pi}_j h_j}{\tilde{\pi}_4 h_4 + \tilde{\pi}_5 h_5 + \tilde{\pi}_6 h_6 + \tilde{\pi}_7 h_7 + \tilde{\pi}_8 h_8} \\ &= .972 \cdot \tilde{\pi}_j h_j \times 10^{-6}. \end{aligned} \tag{2.34}$$

From (2.29) and (2.33), the steady-state probability is calculated as

$$\pi = [.009439, .05607, .009345, .009251, .9159]. \tag{2.35}$$

2.3.2 Password Model for Servers

The example password model based on the original establishment [25] is defined as follows based on the GSPN representation:

$$
\begin{aligned}
\text{GSPN} &= \{P, T_1, T_2, A, W, M_0\} \\
P &= \{p_1, p_2, p_3, p_4, p_5, p_6\} \\
T_1 &= \{t_1, t_2, t_4, t_5\}; \\
T_2 &= \{\tau_3, \tau_6, \tau_7, \tau_8\} \\
W &= \{w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8\} \\
M_0 &= (1, 0, 0, 0, 0, 0),
\end{aligned}
$$

where

- The place, p_1 denotes the initiation of the password cracking of local SCADA systems.
- The place, p_2 denotes the successful login.
- The place, p_3 denotes the failed login to the local SCADA.
- The place, p_4 denotes the knowledge discovered from the SCADA.

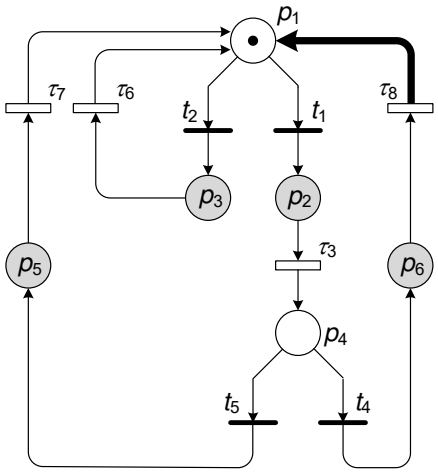
- The place, p_5 denotes the executed sequence of disruptive switching attacks from the SCADA.

- The place, p_6 denotes the failure to sequentially execute switches due to interlocking blocks.

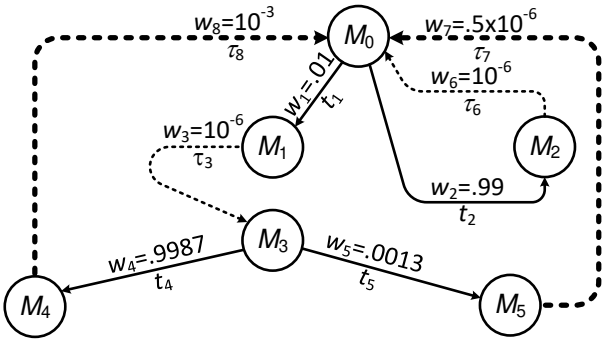
- Variables, t_1, t_2, t_4, and t_5 denote the transition *probabilities* of the successful login to the SCADA, of failure to login to the SCADA, of failing to execute, and of successful execution of the sequential switching in the targeted substation, respectively.

- Variables, τ_3, τ_6, τ_7, and τ_8 denote the transition *rates* of learning to discover the cyber-physical relation, the response to attackers indicating the failed login, response to attackers about successful switching attacks, and response to attackers indicating the failure of the sequential switching due to interlock rules, respectively.

The GSPN and corresponding reachability graph are shown in Fig. 2.15. Once the reachability graph is obtained, the transition *probability* matrix $\mathbf{P}$ and its reduced form $\mathbf{P}'$ are



(a) Petri net model



	p_1	p_2	p_3	p_4	p_5	p_6		
M_0=	1	0	0	0	0	0	M_3=	0 0 0 1 0 0
M_1=	0	1	0	0	0	0	M_4=	0 0 0 0 0 1
M_2=	0	0	1	0	0	0	M_5=	0 0 0 0 1 0

(b) Reachability graph

Figure 2.15: Modified password model [21]

$$\mathbf{P} = \left(\begin{array}{cc|cccc} 0 & 0 & .01 & .99 & 0 & 0 \\ 0 & 0 & 0 & 0 & .9987 & .0013 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \end{array}\right), \tag{2.36}$$

and

$$\mathbf{P}' = \begin{pmatrix} 0 & 0 & .9987 & .0013 \\ .01 & .99 & 0 & 0 \\ .01 & .99 & 0 & 0 \\ .01 & .99 & 0 & 0 \end{pmatrix}_{(4\times 4)}, \tag{2.37}$$

respectively. Using similar argument as in Section 2.3.1, the steady-state distribution, $\tilde{\pi}$, and the steady-state probability, π, are derived as follow:

$$\tilde{\pi} = [.00990 \;\; .9802 \;\; .00989 \;\; .000013], \tag{2.38}$$

$$\pi = [.0099996 \;\; .98996 \;\; .000010 \;\; .000026]. \tag{2.39}$$

2.3.3 IED Authentication (Extended Password Model)

The example password model is also enhanced based on the original establishment [25] in order to implement the two -step authentication function. Below is the tuple of the cyber-net representation to quantify the statuses with transitions representing the model:

$$
\begin{aligned}
\text{GSPN} &= \{P, T_1, T_2, A, W, M_0\} \\
P &= \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9\} \\
T_1 &= \{t_1, t_2, t_5, t_6, t_8, t_9\}; \\
T_2 &= \{\tau_3, \tau_4, \tau_7, \tau_{10}, \tau_{11}, \tau_{12}\} \\
W &= \{w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8, w_9, w_{10}, w_{11}, w_{12}\} \\
M_0 &= (1, 0, 0, 0, 0, 0, 0, 0, 0)
\end{aligned}
$$

where

- The place, p_1 denotes the initiation of password crackings of IEDs.
- The place, p_2 and p_3 denote the failure to access and the successful access to the IED with the viewing mode, individually.

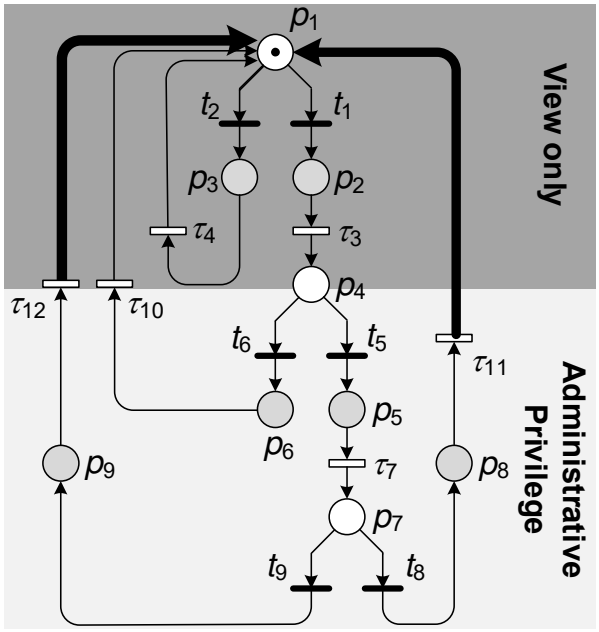
- The place, p_4 denotes the attempt to access to the IED with the control mode.
- The places, p_5 and p_6 denote the failure to access and the successful access to the IED with the control mode, individually.
- The place, p_7 denotes obtaining the knowledge to manipulate IEDs.
- The place, p_8 denotes the executed sequence of disruptive switching actions via IEDs.
- The place, p_9 denotes the failure to execute switching actions due to the maintenance.
- Variables t_1 and t_2 denote transition *probabilities* of the successful access to IEDs with the viewing mode and of the failed access due to wrong passwords, respectively.
- Variables, t_5 and t_6 denote transition *probabilities* of the successful access to IEDs with the control mode and of the failed access due to wrong passwords, respectively.
- Variables, t_8 and t_9 denote the transition *probability* of the successful execution of sequential switching actions of circuit breakers in the targeted substation via the IED and of failing to execute the operation of the IED.
- The variable, τ_3 denotes the transition *rate* of exploring available IEDs with the control mode.
- Variables, τ_4 and τ_{10} denote the transition *rate* of the response to attackers indicating the failed attempt to access to the IED.
- The variable, τ_7 denotes the transition *rate* of learning to discover the knowledge of how to manipulate relay settings of IEDs.

- The variable, τ_{11} denotes the transition *rate* of the response to attackers about successful switching attacks.

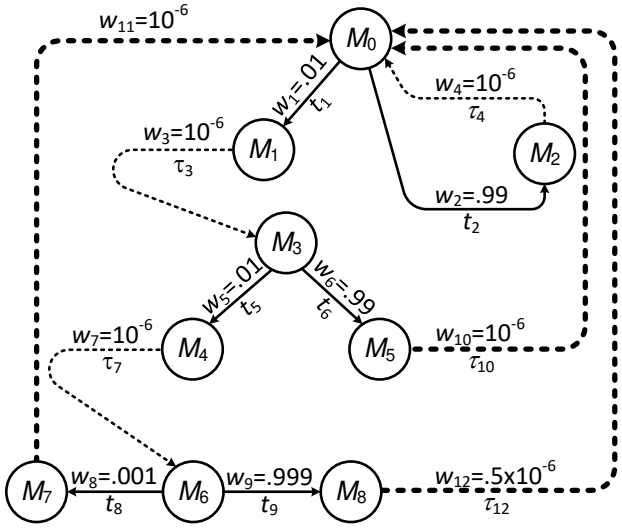
- The variable, τ_{12} denotes the transition *rate* of the response to attackers indicating the out of service state.

Once the reachability graph is obtained, the transition probability matrix is derived as (2.40) and its reduced form is derived as (2.41).

$$\mathbf{P} = \left(\begin{array}{ccc|cccccc} 0 & 0 & 0 & .01 & .99 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & .01 & .99 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & .001 & .999 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)_{(9\times 9)}, \tag{2.40}$$



(a) Petri net model



	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9
M_0	1	0	0	0	0	0	0	0	0
M_1	0	1	0	0	0	0	0	0	0
M_2	0	0	1	0	0	0	0	0	0
M_3	0	0	0	1	0	0	0	0	0
M_4	0	0	0	0	1	0	0	0	0
M_5	0	0	0	0	0	1	0	0	0
M_6	0	0	0	0	0	0	1	0	0
M_7	0	0	0	0	0	0	0	1	0
M_8	0	0	0	0	0	0	0	0	1

(b) Reachability graph

Figure 2.16: IED model [21]

$$\mathbf{P}' = \begin{pmatrix} 0 & 0 & .01 & .99 & 0 & 0 \\ .01 & .99 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & .001 & .999 \\ .01 & .99 & 0 & 0 & 0 & 0 \\ .01 & .99 & 0 & 0 & 0 & 0 \\ .01 & .99 & 0 & 0 & 0 & 0 \end{pmatrix}_{(6\times 6)} . \tag{2.41}$$

The corresponding steady-state distribution and the steady-state probability are derived as (2.42) and (2.43), respectively.

$$\tilde{\pi} = [9900.0, 980100.0, 99.0, 9800.0, .1, 98.9] \times 10^{-6}, \tag{2.42}$$

$$\pi = [9899.0, 980004.0, 99.0, 9800.0, .1, 197.8] \times 10^{-6}. \tag{2.43}$$

2.3.4 Honeynet Model

2.3.4.1 Brief History of Honeynet

There is an inevitable attack, no matter how cybersecurity is reinforced. That is what we call, zero-day attack. This type of attack is characteristic that the hacker can compromise servers before applying the patch to the server. In this case, even the dynamic patch cannot prevent it.

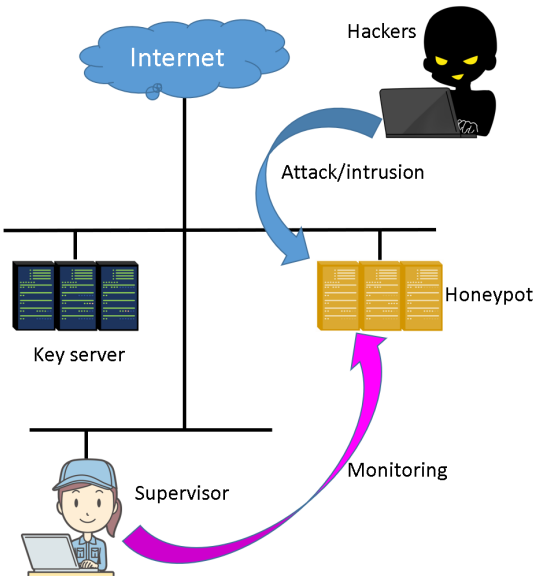


Figure 2.17: Example deployment of honeynet

A honeypot can be a promising tool to make the patch more promptly. A honeypot is a decoy that pretends to be a real server. It is placed with the critical servers, and it allows attackers to invade the honeypot, as shown in Fig. 2.17. Because the attackers usually start downloading their tools and applications to the honeypot after they invade it, what attackers are doing via the honeypot can be observed mostly using event logs.

However, honeypot has not been treated as a useful tool as the security technology. The biggest issue is that the honeypot can be the stepping stone server. That means the honeypot can be used to attack other servers more effectively. The second most significant issue is that it is not easy to operate the honeypot. The professional who can check the attacker's activities and analyze the logs cannot always be hired. On the other hand, the attacker's approaches have been evolved from day today. Honeynet

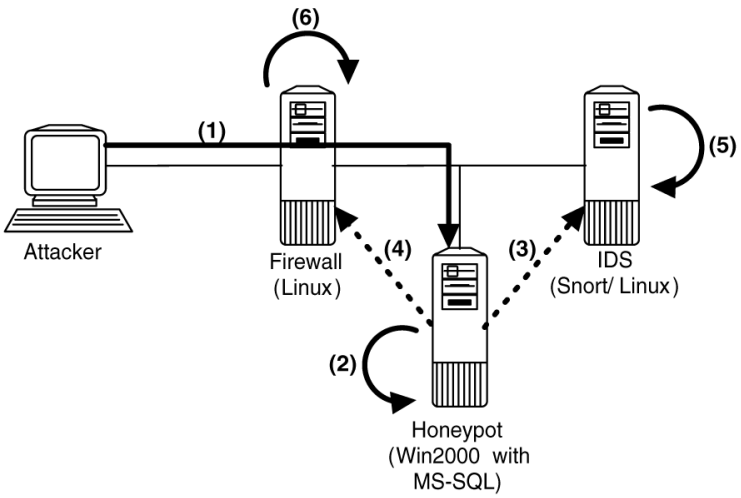


Figure 2.18: Example of prevention function of honeynet [115]

must be more highlighted because it helps to enhance situational awareness.

A prevention function that is shown in Fig. 2.18can be a promising way to tackle the first issue.

2.3.4.2 Modeling of Honeynet

The proposed cyber-net model contains the modified password model and the IED model in the previous section, as well as the developed honeynet model. The honeynet is assumed to have the following functions:

- Collect passwords
- Update the firewall rule to prevent the attackers from connecting to the Internet from the honeynet.

Generally, a honeypot should trap intruders that establish security events where such anomalies would be their footprints across a network. The logging features are captured in the cyber-net modeling, where it can interact with firewalls within the network to coordinate substation's anomaly events. Such events can reflect new rules at the time and will thwart future intruders. The observed statistics stay in the event logging that can be purged once every audit cycle. The modeling of a particular type of honeypots can mimic the IEDs, where attackers may use it as a steppingstone to further a plot. In the case of honeynets with the prevention function in Fig. 2.18, the firewall can automatically update the statistics reflecting the new rules that can mitigate in the next cycle of observations as evidence for NERC CIP.

2.3.4.3 Integrated Cyber-net Model with Honeynet

The example cyber-net model with honeynets are shown in Fig. 2.19. The following immediate or timed transitions are used in the GSPN model:

- Variables, t_1 and t_2 denote transition *probabilities* of the intrusion attempt for the honeypot and IEDs, respectively.

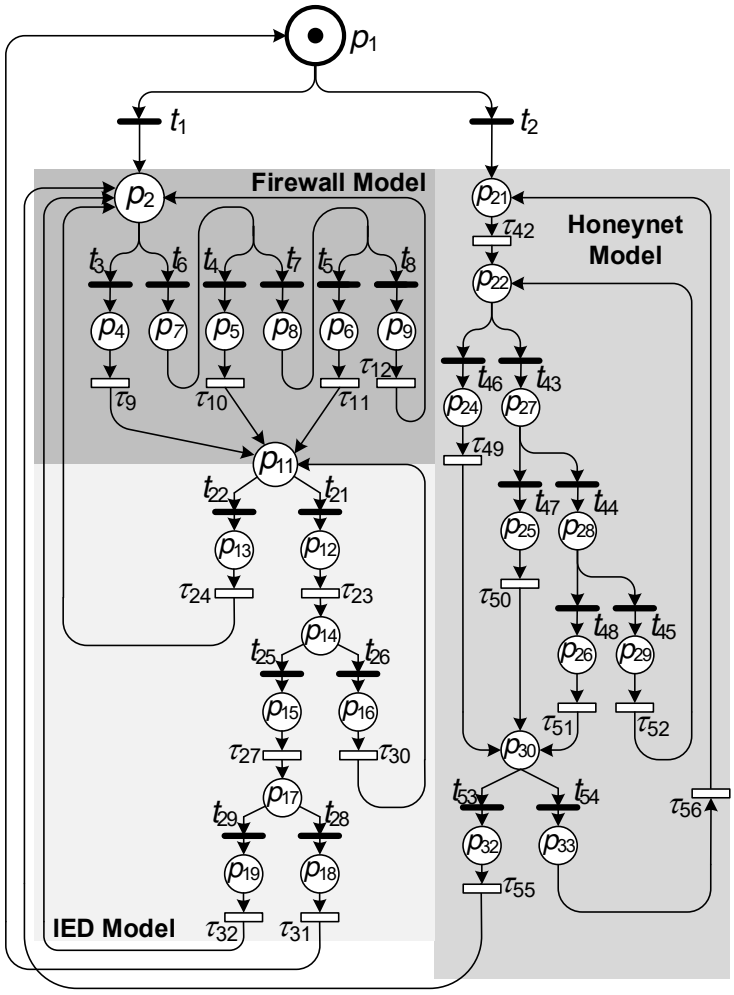


Figure 2.19: Petri net model for cyber-net with honeynet [21]

- Variable, τ_{42} denotes the transition *rate* of copying the tools to the honeynet for the intrusion attempt.
- Variables, t_{43} through t_{45} denote transition *probabilities* of the failure to crack a designated firewall rule.
- Variables, t_{46} through t_{48} denote transition *probabilities* of the successful cracking of firewall rules.
- Variables, τ_{49} through τ_{51} denote transition *rates* of responding to attackers opening

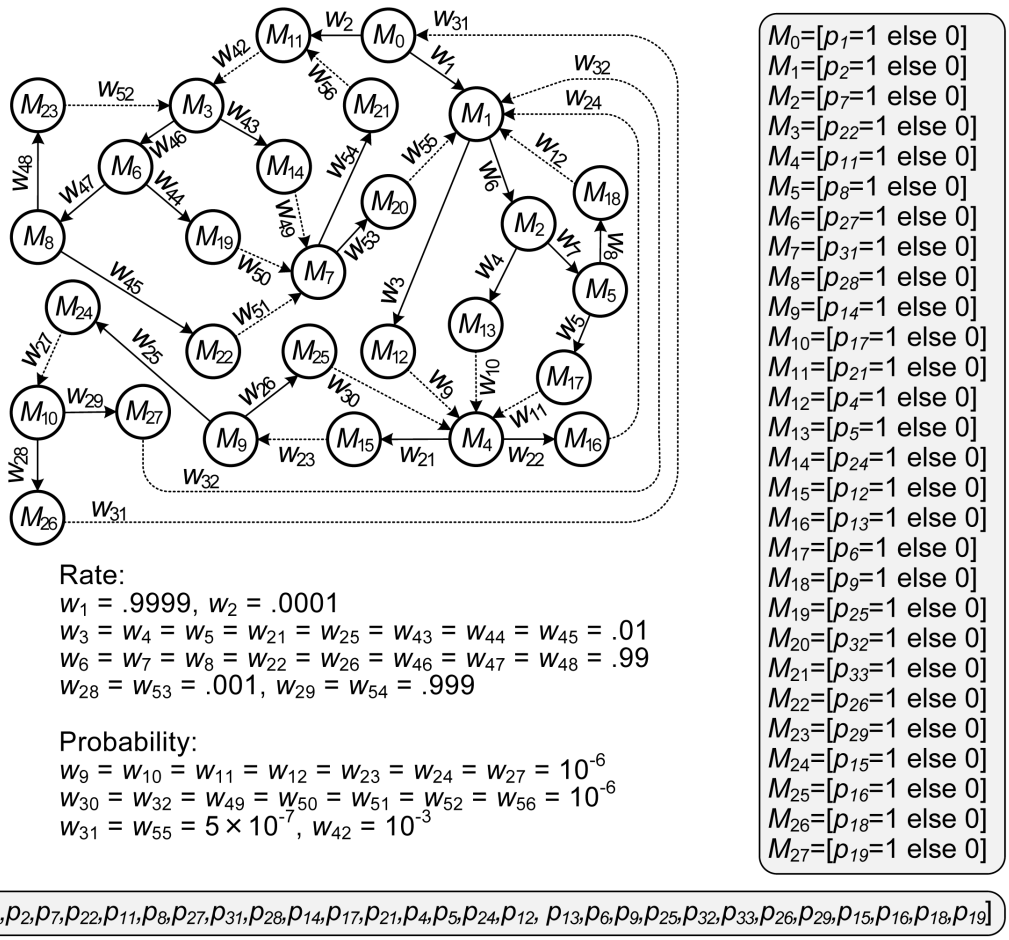


Figure 2.20: Reachability graph for cyber-net with honeynet [21]

a designated port. Variable.

- The variable, τ_{52} denotes the transition *rate* of response to the attackers indicating failure to open any ports.
- Variables, t_{53} and t_{54} denote transition *probabilities* of the successful communication to the Internet from the honeynet and of the failure to communicate to the Internet from the honeynet, respectively.
- Variables, τ_{55} and τ_{56} denote the transition *rate* of exploring the available IED and of failure to reaching to the IED due to the prevention function that are

implemented in the advanced honeynet, respectively.

It is noted that the rest of the transition probabilities and rates in the firewall model and the IED model have been defined in the previous sections, 2.3.1 and 2.3.3.

Chapter 3

Case Studies of Intrusion Paths to Substation Networks

3.1 Model Parameters and Insights from Steady-State Probabilities

The developed cyber-net model enables to derive several useful indicators. The steady-state probability of cracking the firewall is calculated from the sum of the probabilities of p_{12} and p_{13}. The steady-state probability of cracking the first authentication is calculated from the sum of the probabilities of p_{15} and p_{16}. The steady-state probability of cracking the second authentication is calculated from the sum of the

probabilities of p_{18} and p_{19}. The steady-state probabilities of disruptive switching actions and of the successful transmission of the outgoing packets from the honeynet to attack other servers, (*i.e.*, using the honeynet as the steppingstone) are obtained from p_{18} and p_{32}, respectively.

The first clause introduces sensitivity analyses for honeynet using the developed cyber-net model in Fig. 2.19. The second clause provides the steady-state probabilities of the substation outages due to disruptive switching attacks for SCADA and IEDs using the IEEE 14-bus system model [46]. The attack from outside is assumed for all the case studies.

3.2 Sensitivity Analysis of Intrusion Attempts with a Single IED

3.2.1 Integrated Models with Honeynets

The steady-state probabilities of each place in Fig. 2.19 are shown in Table 3.1. The steady-state probability of disruptive switching actions is 5.8×10^{-9}. The steady-state probability at the place, p_9 gives the highest value of 0.94. The steady-state probability at the place, p_{13} gives the second highest value of 0.029. These results show

Table 3.1
Probabilities of a cyber-net in Fig. 2.19

Place	Probability	Place	Probability
P04	9.70590E-03	P19	2.90866E-06
P05	9.60884E-03	P21	2.91186E-13
P06	9.51275E-03	P24	9.80392E-11
P09	9.41763E-01	P25	9.70589E-11
P12	2.91157E-04	P26	9.60883E-11
P13	2.88246E-02	P29	9.51274E-09
P15	2.91157E-06	P32	5.82373E-13
P16	2.88246E-04	P33	2.90895E-10
P18	5.82315E-09		

that most attackers are highly likely to keep attempting the firewall rule cracking. Historical data are often used to estimate the future cyber-risk. However, invisible/implicit risks such as cracking the firewall cannot be estimated. The proposed cyber-net model enables to derive such risks as the steady-state probabilities.

The steady-state probabilities of disruptive switching attacks with honeynets that do not have the prevention function, and with advanced honeynets that have the prevention function are derived and compared in this case study. In the case of the honeynet with no prevention function, the transition probabilities, t_{53} and t_{54} are set as 0.999999 and 1.0×10^{-6}, respectively. In the case of theh advanced honeynet, the transition probabilities, t_{53} and t_{54} are set as 1.0×10^{-6} and 0.999999, respectively. The fraction of the honeynet is set as the transition probability of t_2 in the range of 0 (0%) and 1, (100%) and five indicators are shown in Figs. 3.1 and 3.2. As shown in Fig. 3.1, the steady-state probability of reaching the Internet from honeynets linearly

increases as the fraction of honeynets increase, while four steady-state probabilities with honeynets that have no prevention function are almost the same regardless of the fraction of honeynets. On the other hand, Fig. 3.2 shows five steady-state probabilities with advanced honeynets. The curve in the figure shows exponential changes with respect to the increased number of honeynets and servers deployed in the substation network.

The following are the observations from the simulation with or without prevention function:

3.2.2 Honeynet without Prevention

As depicted in Fig. 3.3, the discrete events from simulations show the two distinct curves of probabilities for each events where all of them converge in the end. If the honeynet without prevention function shares 99% of the servers, the number of attackers who spread outgoing packets gradually increases as time goes (see the second top indicator in Fig. 3.3). That results in an increased number of attackers who attempt to crack firewall rules, *i.e.*, where steady-state probabilities of places, p_4, p_5, p_6, p_9, rise consistently when it reaches the steady state.

At the time of around 10^7, the place describing the attackers crowding to the password cracking stage via successfully cracking firewall rules (see the third top indicator in

Fig. 3.3). Although the increasing timings of the third top indicator are different depending on the fraction of honeynets, the third top indicator eventually reaches to the same level over a long period of time. Because steady-state probability only indicates the probability over the long period of time, steady-state probabilities of cracking firewall rules and passwords and of switching attack are the same, independent from the total numbers of honeypots and servers are modeled.

3.2.3 Honeynet with Prevention

If the honeynet has the prevention function, nearly all attackers are trapped in the honeynet (*i.e.*, such attackers fail to infect other servers from the honeynet) once they invade into it. That implies that the honeynet model has a dead end that does not feedback to the attackers as part of the learning process. On the other hand, the IED model has a feedback that enables attackers learn in this trial-and-error discovery. That says, some attackers who successfully perform the switching attack can be trapped in the honeynet at the second round or later according to the hypothesized fraction of t_2. Because the steady-state probability discusses the probabilities of each state over an incredibly long period of time, no loop structure of the honeynet model makes the number of attackers who are trapped in honeynets exponentially accelerated as the fraction of honeynets, t_2 increases. Then, the number of such attackers is saturated once the probability of the switching attack is small,

contributing insignificantly to the overall risk.

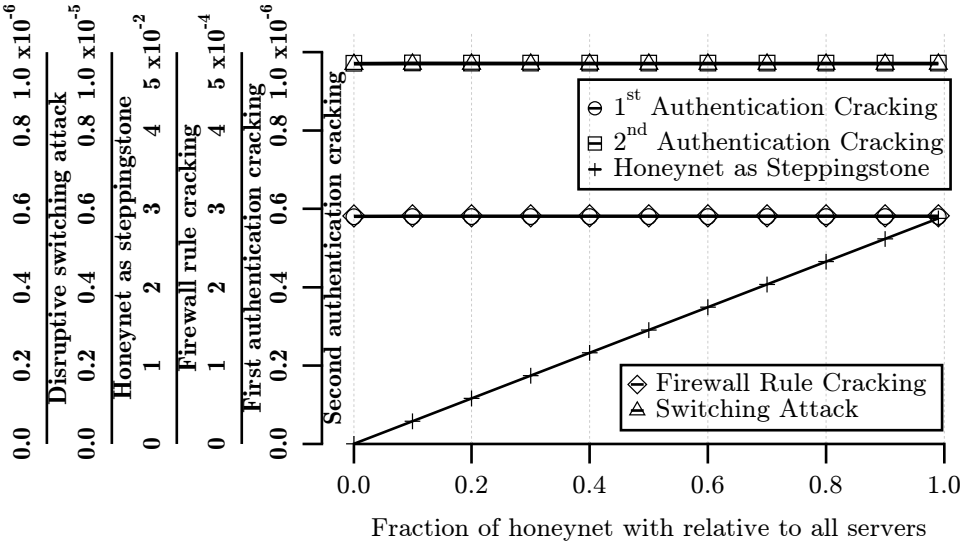


Figure 3.1: Probabilities of a cyber-net in response to fraction of honeynet without prevention function [21]

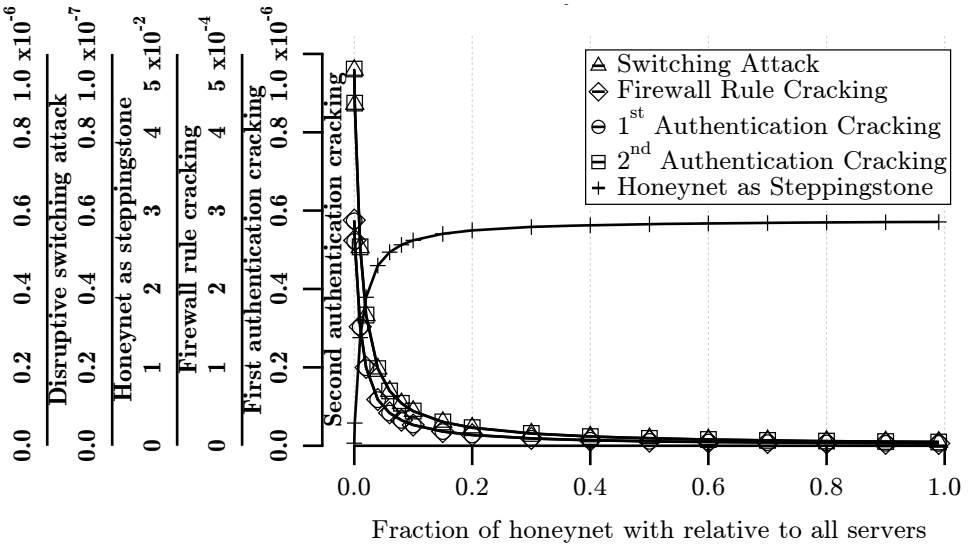


Figure 3.2: Probabilities of a cyber-net in response to fraction of honeynet with prevention function [21]

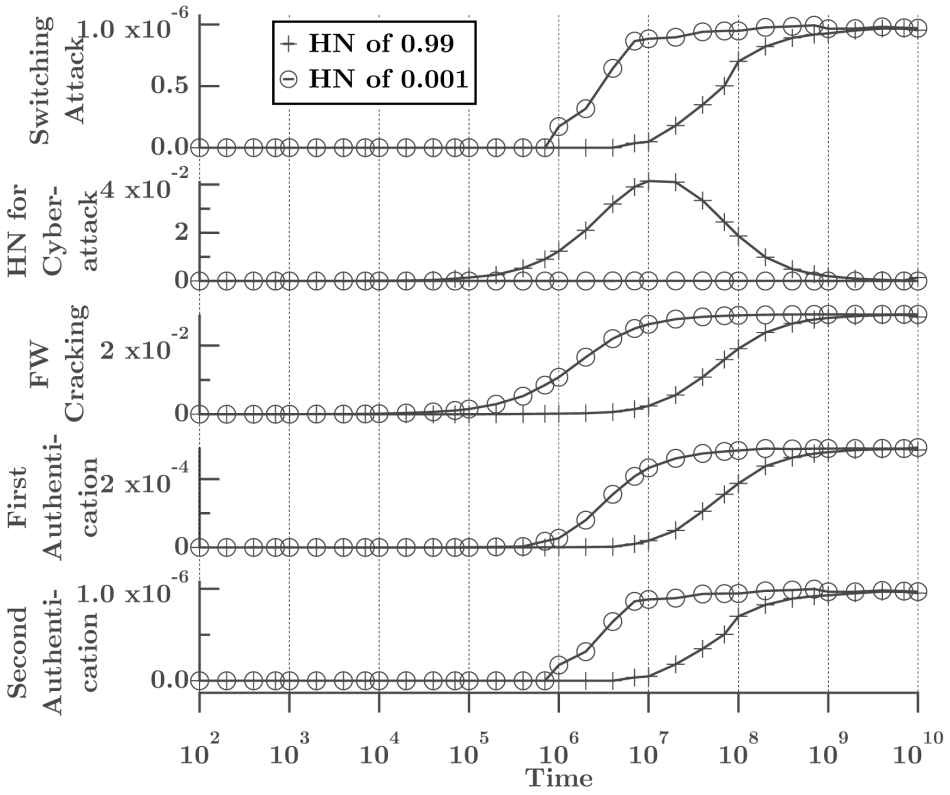


Figure 3.3: Time-varying probabilities of a cyber-net in response to fraction of honeynet without prevention function [21]

3.3 Sensitivity Analysis with Multiple Systems

To reach the steady-state probability of substation attacks, the cyber-net model in Fig. 2.19 is further extended to include multiple IEDs and a SCADA. The major protections that are installed at 220 kV or over substations and power stations are taken into account as IEDs. Readers can refer to the typical representation of relay types and the number of their settings per each relay in substations from [116]. This reference of the CIGRE report based on the relay experts from around the world is used as the base to set up the case studies here. We deem the number of setting

parameters on relaying as potential combinations of tripping associated breaker(s) by experience. This reference is used here in the simulation study.

3.3.1 Interpretation of Immediate Transitions

The installed protections are different between a power station and a substation, and the volume of these protections at each power station/substation varies depending on the number of power equipment such as generators, transformers, buses, and transmission lines. In addition, the type of protective relays can vary depending on the voltage level in the substation.

A distributed control center monitors and controls 6-7 substations in transmission systems on average, according to the real-world example. If the distributed control centers are modeled at a 132kV/66kV substation in the IEEE 14-bus system model, two control centers are hypothesized. Because IEDs and the server at the control center have their unique static IP addresses, the risk of the substation attacks via a control server can be diversified at a substation level.

In this study, each relay type is assigned to individual IED, and t_{21} and t_{22} in Fig. 2.19 are provided according to the fraction of the protective relays at a substation,

as shown in Eqs. (3.1) and (3.2).

$$t_{21,\text{IED}} = \frac{0.01 \times \sum_{j=1}^{n_{\text{relay}}} j}{\sum_{i=1}^{n_{\text{relay}}} i + \frac{n_{\text{CS}}}{n_{\text{SS}}}}; \quad t_{21,\text{SCADA}} = \frac{0.01 \times \frac{n_{\text{CS}}}{n_{\text{SS}}}}{\sum_{i=1}^{n_{\text{relay}}} i + \frac{n_{\text{CS}}}{n_{\text{SS}}}} \tag{3.1}$$

$$t_{22,\text{IED}} = \frac{0.99 \times \sum_{j=1}^{n_{\text{relay}}} j}{\sum_{i=1}^{n_{\text{relay}}} i + \frac{n_{\text{CS}}}{n_{\text{SS}}}}; \quad t_{22,\text{SCADA}} = \frac{0.99 \times \frac{n_{\text{CS}}}{n_{\text{SS}}}}{\sum_{i=1}^{n_{\text{relay}}} i + \frac{n_{\text{CS}}}{n_{\text{SS}}}} \tag{3.2}$$

where n_{relay} denotes the number of same relay type at a substation, n_{CS} and n_{SS} denote the numbers of control centers and substations in the system, respectively ($n_{\text{CS}} = 2$ and $n_{\text{SS}} = 10$ for this study case).

3.3.2 Timed Intrusion Transitions

This paper proposes a systematic manner of how to provide two specific parameters, τ_{27} and τ_{31} of the developed cyber-net model in Fig. 2.19. When an IED is compromised by attackers, and the relay settings change, malicious tripping due to the intentional wrong relay settings could occur. In this case, the time to review all relay settings is highly likely to increase as the number of relay settings increases. It is suggested that the time to learn how to deal with the IED for the attack, *i.e.*,

the inverse of τ_{27}, is assumed to be proportion to the number of relay settings for each protection scheme. In this case study, τ_{27} is set as the default imputed value of 1.0×10^{-6} for the IED, *i.e.*, the distance relay that has the largest number of relay settings of 19 and derived from Eq. (3.3). The transition rate τ_{27} for SCADA needs to be initialized as there is a much larger number of switches to be reviewed, it is likely to have a longer time to overview all controllable switches and to get acquainted with the environment of local SCADA system than direct connections to IEDs. In this study, τ_{27} for SCADA is set to be 9.5×10^{-8}.

On the other hand, at least one AND conditions and many OR conditions are generally included in the relay logic diagram, and many relay settings can be restrained to avoid the improper relay settings coordination. Therefore, as the number of relay settings increases, the possibility of the malicious relay operation can increase against such constraints, *i.e.*, the attackers are likely to shorten the time to operate the targeted IED. In light of this, it is suggested that the time to complete disruptive switching actions, *i.e.*, the inverse of τ_{31} may be assumed to be inversely proportional to the number of relay settings. In this case study, τ_{31} is set as the default imputed value of 0.5×10^{-6} for the IED, *i.e.*, the high impedance voltage differential relay that has the smallest number of relay settings of 2 and all τ_{31} are derived from Eq. (3.3). In this study, τ_{31} for SCADA is set to be 4.17×10^{-7}.

$$\tau_{27,\mathrm{IED}} = \frac{1.0 \times 10^{-6} \times 19}{n_{\mathrm{ry\_set}}};\ \tau_{31,\mathrm{IED}} = \frac{0.5 \times 10^{-6} \times n_{\mathrm{ry\_set}}}{2} \tag{3.3}$$

where $n_{\text{ry\_set}}$ denotes the number of relay settings.

The rest of the transition parameters are assumed to be the same as the values in Fig. 2.19. These will be updated based on the observation of the time window from the available event source from the local computer systems.

3.3.3 Typical System Deployment in Substation and Case Studies

Figure 3.4 shows the outline of the created cyber-net model with up to 8 IEDs. In order to elaborate on the installed protections at each power station/substation, the following are considered using [46]:

- A step-up transformer of synchronous generators or condensers are directly connected to the 132-kV bus; they are typically connected to a substation with the voltage level is lower than 132-kV. Step-down transformers of loads are not considered in this study.
- One reactive power compensator is included if a load or a transformer is explicitly shown without reactive power compensators or synchronous condensers.
- A double-circuit line for the one-line diagram shown in general IEEE test cases. Advanced line protection that compensates for the zero-phase circulation current

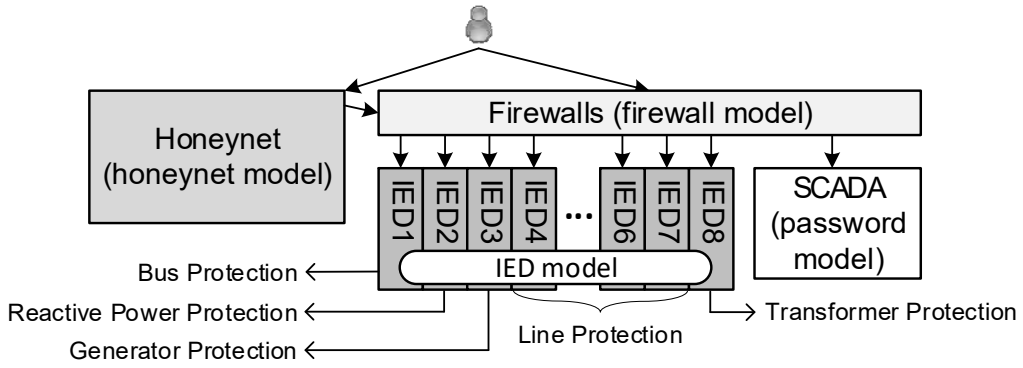


Figure 3.4: Case setup for cyber-net with multiple protective IEDs and a SCADA [21]

is assumed to be applied to multi-circuit transmission lines that share the same towers.

3.3.4 Simulation Results

The probabilities of disruptive switching executed against the substation automation SCADA system or executed by compromised IED-initiated (CII) attacks are shown in Table 3.2. The table shows that the probabilities of IEDs are inversely proportional to the number of relay settings as well as proportional to the number of protective relays, relatively to all relays in the designated substation.

The steady-state probability of the substation attack is the summation of the steady-state probabilities of switching attacks for the SCADA and for IEDs that result in

the entire substation outage. A subset of breaker tripping associated IEDs can energize the entire substation, depending on the substation topology. For example, compromising IED6 and IED7 at Bus 1 in Table 3.2 can cause the whole substation outage. The steady-state probability of such a simultaneous switching attack is calculated using two initial tokens. In this case, the steady-state probability of the switching attack for IED6 and IED7 is derived as 1.70×10^{-14}, which is 10^4 times smaller than the steady-state probability of switching attacks for the SCADA and negligible. On the other hand, compromising IED1 at Bus 1 in Table 3.2 also causes the whole substation outage. This steady-state probability is around 100 times larger than that for the SCADA and is not negligible. Therefore, the only steady-state probability of switching attacks for a single IED that causes the whole substation attack, (*i.e.*, only when all bus protections at a substation are compromised) other than the steady-state probability for the SCADA needs to be included. In other words, the steady-state probability of switching attacks can be negligible when using more than or equal to two different relay types for bus protections. In this case study, the steady-state probability of the switching attack for substation 1 at Bus 1 can be derived as 1.592×10^{-7}(with $1.563 \times 10^{-7} + 2.927 \times 10^{-9}$). The same procedure is applied to derive the steady-state probability of switching attacks at each substation in the different IEEE standard models, such as IEEE 30-Bus [117], 57-Bus [65], and 118-Bus systems [66] as shown in Table 3.3 and Fig. 3.7.

Table 3.2
Steady-state probabilities of substation attack for IEEE 14-Bus system
with hypothesized relay types

	Substation										Protection type	Relay type	Number of relay settings
	Bus 1	Bus 2	Bus 3	Bus 4 Bus 9	Bus 5 Bus 6	Bus 10	Bus 11	Bus 12	Bus 13	Bus 14			
IED1	1.563E-07 (1)	1.182E-07 (1)	1.864E-07 (1)	1.729E-07 (2)	1.953E-07 (2)	2.307E-07 (1)	2.307E-07 (1)	2.307E-07 (1)	1.864E-07 (1)	2.307E-07 (1)	Bus	Current differential	12
IED2	N/A	N/A	N/A	2.075E-07 (1)	N/A	5.537E-07 (1)	5.537E-07 (1)	5.537E-07 (1)	4.473E-07 (1)	5.537E-07 (1)	Reactive power compensator		5
IED3	1.443E-07 (1)	1.091E-07 (1)	1.720E-07 (1)	7.981E-08 (1)	9.013E-08 (1)	N/A	N/A	N/A	N/A	N/A	Generator		13
IED4	N/A	N/A	N/A	2.075E-07 (2)	N/A	N/A	N/A	N/A	N/A	N/A	Sub-transmission line (multi-circuit)	Advanced transverse differential	10
IED5	N/A	N/A	N/A	N/A	5.858E-07 (3)	9.228E-07 (2)	9.228E-07 (2)	9.228E-07 (2)	1.118E-06 (3)	9.228E-07 (2)	Sub-transmission line	Transversal differential	6
IED6	3.411E-07 (2)	5.158E-07 (4)	N/A	1.886E-07 (2)	2.130E-07 (2)	N/A	N/A	N/A	N/A	N/A	Transmission line (multi-circuit)	Advanced current differential	11
IED7	4.689E-07 (1)	3.546E-07 (1)	1.118E-06 (2)	2.594E-07 (1)	2.929E-07 (1)	N/A	N/A	N/A	N/A	N/A	Transmission line	Current differential	4
IED8	1.876E-07 (1)	1.418E-07 (1)	2.236E-07 (1)	2.075E-07 (2)	1.172E-07 (1)	N/A	N/A	N/A	N/A	N/A	Transformer	Current differential	10
SCADA	2.927E-09	2.213E-09	3.489E-09	1.619E-09	1.828E-09	4.320E-09	4.320E-09	4.320E-09	3.489E-09	4.320E-09	N/A	N/A	N/A
Total	1.592E-07	1.204E-07	1.899E-07	1.745E-07	1.971E-07	2.350E-07	2.350E-07	2.350E-07	1.899E-07	2.350E-07	N/A	N/A	N/A

Note: figures in brackets denote the number of protective relays

Table 3.3
Relay modeling: types and settings using four IEEE standard system models

IEEE standard system model	14-bus	30-bus	57-bus	118-bus
Number of substation (and power station)	10	24	43	109
Number of SCADA	2	3	4	11
Relay type of high-voltage line protection	Ordinary current differential (4); Advanced current differential (11)			
Relay type of medium-voltage line protection	Ordinary transversal differential (6); Advanced current differential (10)			
Relay type of low-voltage line protection	N/A	N/A	Distance (19)	N/A
Relay type of bus protection for substation	Current differential (12)			
Relay type of bus protection for switching station	High-impedance voltage differential (2)			
Relay type of transformer protection for step-up transformer	Current differential			
	(12)	(12)	(12)	Synchronous generator (12) Synchronous condenser (13)
Relay type of transformer protection for step-down transformer	Current differential			
	(12)	(12)	Autotransformer (13) Ordinary transformer (14)	(14)

Note: figures in brackets denote the number of relay settings for the corresponding relays.

Table 3.4
Measure of derivation of transition probability and rate for substation attack with used values for IEEE 14-Bus system

Transition probability/rate	Measure of setting transition probabilities and rates	Example of reference source	Values for case study
$t_1(=1-t_2)$	Number of honeypot servers with relative to all control servers including honeypot servers	Brochure for control centers	0.0001
$t_3(=1-t_6)$, $t_4(=1-t_7)$, $t_5(=1-t_8)$, $t_{43}(=1-t_{46})$, $t_{44}(=1-t_{47})$, $t_{45}(=1-t_{48})$.	Number of successful attempts to open a port with relative to the total attempts to open the port	Operating system event logs	0.01
τ_9, τ_{10}, τ_{11}, τ_{49}, τ_{50}, τ_{51}.	Inverse of the following sum of the averaged time 1) response time to attempt opening the port 2) response time to confirm that the status of the port is opened 3) response time to reach to the password input screen of the targeted server 4) response time to input the first password	Specification of server performance	1.0×10^{-6}
τ_{12}, τ_{52}	Inverse of the following sum of the averaged time 5) response time to attempt opening the port 6) response time to confirm that the status of the port is closed		1.0×10^{-6}
τ_{23}	Inverse of the following sum of the averaged time 7) response time to reach to the second password input screen 8) response time to input the second password		1.0×10^{-6}
τ_{24}	Inverse of the averaged response time to return to the first password input screen		1.0×10^{-6}
τ_{30}	Inverse of the averaged time to return to the first password input screen		1.0×10^{-6}
$t_{21}(=1-t_{22})$	9) Number of successful attempts to log in to the targeted server as the first authentication 10) Fraction of one relay type with relative to all relay types at a substation or a power station	Security event logs of servers	0.01 Eqs. (3.1)(3.2)*
τ_{27}	11) Inverse of the averaged time to review and to learn how to change relay settings 12) Fraction of relay settings with relative to maximum/minimum relay settings	Instruction manual of protective relays	1.0×10^{-6} Eq. (3.3)
τ_{31}	13) Inverse of the averaged time to opening all circuit breakers that are connected to a substation 14) Fraction of relay settings with relative to maximum/minimum relay settings		5.0×10^{-7} Eq. (3.3)
$t_{28}(=1-t_{29})$	15) Fraction of IEDs with relative to all protective relays and/or fraction of digitalized substation with relative to all operating substations 16) Fraction of IEDs without interlocking or a function that can cope with the switching attack	In consultation with manufacturers/utilities	0.0001
τ_{32}	Inverse of the averaged time to give up substation attacks from the attack inception	Substation diagram	5.0×10^{-7}
τ_{42}	Inverse of the averaged time to copying tools into the honeynet for the cyberattack	Event logs of honeypot	1.0×10^{-3}
$t_{53}(=1-t_{54})$	Fraction of time between the honeynet infection and application of the newly generated rule	Data sources of security vulnerabilities	0.01
τ_{55}	Inverse of the averaged time to apply the newly generated rule after the honeynet infection		1.0×10^{-3}
τ_{56}	Inverse of the averaged time to fail to send outgoing packets to infect other servers		5.0×10^{-7}

* The value of 9) is reflected in 10), *i.e.*, Eqs. (3.1) and (3.2).

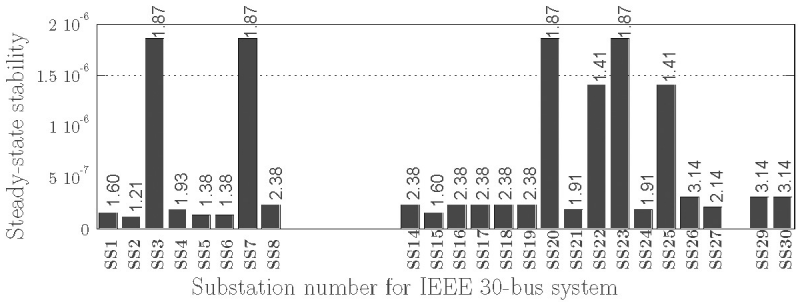


Figure 3.5: Steady-state probability for each substation (sequential order) in IEEE 30-bus systems

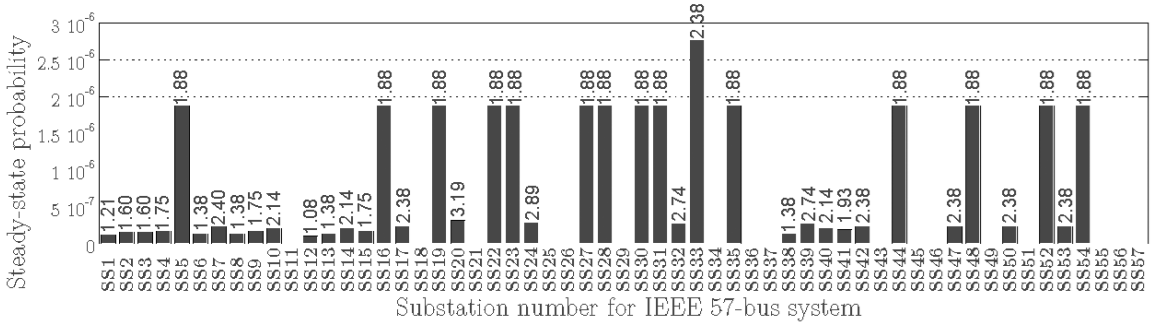


Figure 3.6: Steady-state probability for each substation (sequential order) in IEEE 57-bus systems

3.4 Practical Consideration in Case Studies

3.4.1 Industry Practice in Security Logging

In practice, anomalous statistics for each utility can largely vary. Due to the proprietary information, such datasets are not publicly available. Some values are imputed based on the empirical base that falls within a reasonable range. Although deriving reasonable transition probabilities and rates for the cyber-net model would be a

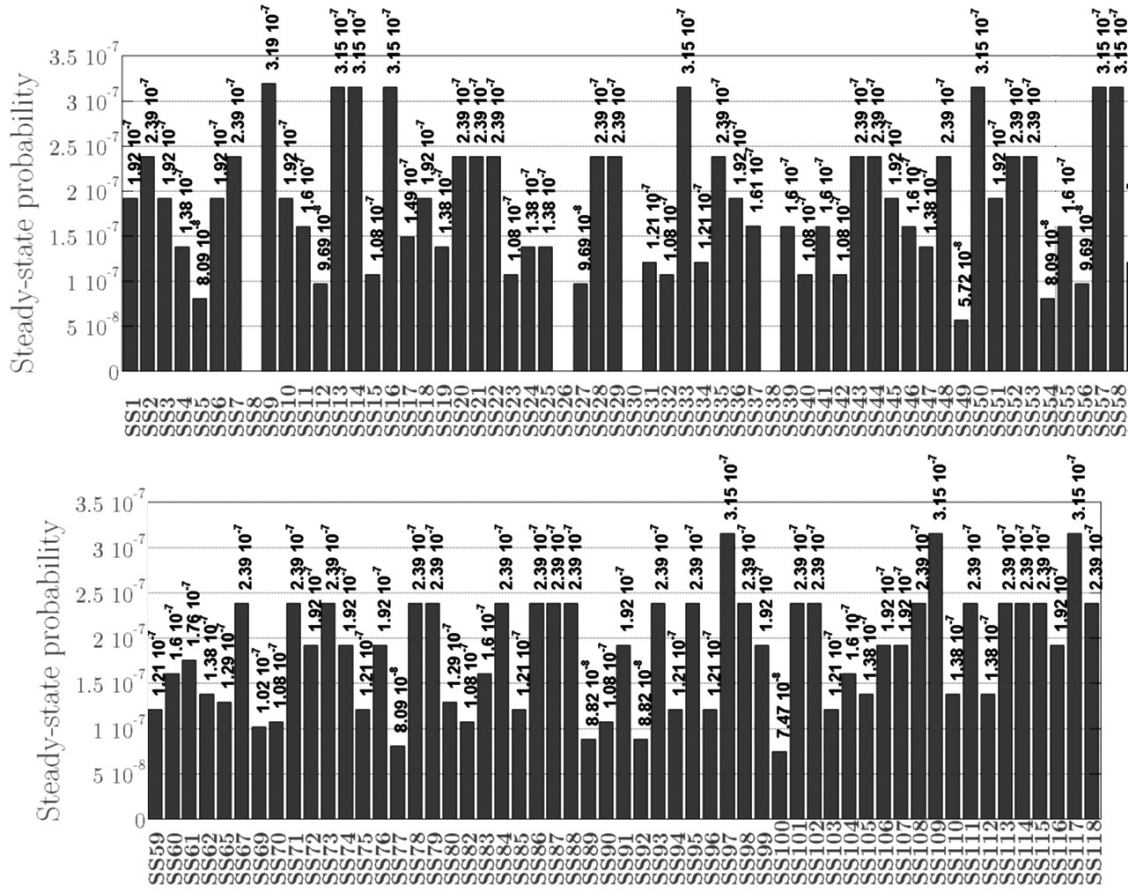


Figure 3.7: Steady-state probability for each substation (sequential order) in IEEE 118-bus systems

future research study, the considerable approach is shown in Table 3.4.

The number of commissioned protective relays set up in substations can be directly obtained from the utilities. This is in proportion to the typical deployment of substation equipment, such as associated busbars, transmission lines, and transformers. The attempts resulting in successful intrusion to bypass firewalls or passwords can be inferred from the security event logs from the available sources. That can include honeypots to be modeled [118, 119, 120]. The frequency of the zero-day attack can

also be obtained from the database that is available to the public [121, 122]. As security event logs do not reveal to the *zero-day* vulnerability for the honeynet and the data can vary as time goes by, only carefully thought values are imputed in the case studies. Accessing to the proprietary data would strengthen the quality of systemic risk in a practical case study that would allow insurances to better assess utility risk with regards to their readiness in security defense.

3.4.2 Transition to Cyber Insurance Business for Power Grids

The creativity of attackers' stratagem can result in different operational implications. Switching attack in the control system would perturb the instability of a power grid. There may be combinations of events with assistance from insiders where an attack can be effective when coordination between insiders and the remote collaborators may create events of disturbance, such as electrical short circuits. Substations are connected with multiple components where an abrupt switching of all of these components can implicate system operation, which is studied in [35, 36, 37, 38]. Although security is viewed as a *low-probability, high-impact* event, the new perspectives of enterprise risk management in planning should consist of two major components, *i.e.*, assessment of security readiness and remedial/preventive responses. The planning

for security investment should be based on the operational bottleneck from historical observations with simulations where it should reflect consequential contingencies associated with each substation and their corresponding outages. On the contrary, this work extensively captures the high level of abstraction with respect to technology implementation, and the events from the first intrusion attempt to execute a switching attack in discrete events successfully. The prevention of such cyber events is described in the proposed models.

3.4.3 Establishing Actuarial Framework

Establishing the premium of an insurance policy depends on two fundamental aspects of consideration, *i.e.*, (1) distributions of frequency, and (2) severity of insurance claims. These two distributions are often estimated based on historical observations. This work establishes a systemic risk framework to provide quantities pertaining to what is deployed in substations. To the best of our knowledge, gauging the frequency of event occurrence that captures within a substation has been challenging due to a large number of attack vector combinations. The proposed model estimating the steady-state probabilities of potential case combinations provides a means of adjustment for future protection improvement in security planning. The anomalous incidents can lead to successful intrusion, and the actuarial aspect of the anomalies should be captured in the systemic risk.

Chapter 4

Simulated Attack Impacts of Grid-Wide Stability

The impact of switching attacks may be simulated by either a power flow-based approach and a dynamic simulation-based approach. The former has been studied in [41, 42]. However, the latter is not studied with sufficient protection models. In power engineering society, N-k contingencies have been carefully examined. Most of the contingencies are system faults with a significant voltage drop and/or frequency drop. In the case of the voltage drop, the ephemeral, transient behavior occurs only during the fault, and then the power grid moves into the post-fault operating point. This short-term (typically 60-250 ms) behavior can accelerate the rotor speed of synchronous generators, and the grid results in the disconnection of generating units

along with the loss of synchronism. Most rotor angle stability studies accompany the aforementioned short-term behavior with significant voltage sags. On the other hand, switching attacks do not possess this type of behavior because the specific system event does not happen. It is noted that the behavior and impact are the same between the frequency-related N-k contingencies and the switching attack that disconnects generators and loads only.

Disconnecting branches opening circuit breakers do not usually cause a significant impact on the power grid. Therefore, this event is not treated as any contingencies. However, if all branches connected to one or more substations are disconnected, this impact can be unignorable. This study is totally out-of-scope in the industry because this is treated as an extremely rare event. Besides, there is no generally accepted guideline of which models power engineers should employ for the simulation.

Chapter 4 clarifies the necessary control models and protection models that must be used for switching attack studies. Transient stability, frequency stability, and voltage stability are considered when extracting the necessary models. The time-domain simulation results for the switching attack against substations and IEDs are showcased using IEEE standard models.

4.1 Key Factors of Dynamical Behaviors

This section discusses the contributing factors of system dynamics that can lead to cascading consequences, leading to potential brownout or blackout.

4.1.1 Voltage Threshold

Voltage level of substations with 200 kV or higher can be vulnerable to switching attacks. Therefore, the transmission network can become the major target and analysis of base case and how the bottleneck of a system can be identified and later implemented with security protection technologies. Although the remove of a lower voltage substation may not initialize a cascade of blackout, the combinatorial analyses should be included in a study.

4.1.2 Types of System Stability

Grid's well-being is observed by its abnormal phenomena that is generalized into 3 types: (1) transient stability, (2) frequency stability, (3) voltage stability, and overload [123]. Any of the stability issues below can occur triggered by the initial events of sequential switching attacks in substations.

Transient stability: Transient stability is not generally violated without the significant voltage drop. Therefore, the possibility of the violation of transient stability due to substation switching attacks is relatively low. However, poorly damped power swing oscillation or negative damping oscillation can happen, when the dominant frequency component of the power swing oscillation totally changes, or when steady-state stability is violated after the substation switching attack. In addition, the angle difference between synchronous generators and synchronous condensers can be expanded during the cascaded events, which results in the out-of-step status in the grid.

Frequency stability: Losing one or more substations due to switching attacks often create abrupt mismatch in power balance between generation and loads, which results in change in the system frequency. In general, as k of "S-k" becomes larger, frequency stability issue is more likely to happen (But that is not always the case). Both significant frequency drop or rise can occur. However, frequency drop is more likely to be observed because the frequency rise leads to the generator tripping by overfrequency protections. This is due to the frequency starts to decrease after the generator tripping.

Voltage stability: Undervoltage load shedding can happen once the significant voltage drop mainly due to system faults or deficiency of the reactive power support. However, some loads are disconnected due to their local protection in the case of low voltage before activation of undervoltage load shedding. In addition,

system faults do not occur during substation switching attacks. Therefore, the voltage collapse caused by voltage stability is unlikely to happen. On the other hand, the significant voltage rise can also happen especially when loads with a large amount of reactive consumption are lost all of a sudden (see a case study in Clause 4.4.2). That condition is likely to happen especially when a large amount of loads and/or transformers are disconnected due to substation switching attacks. As k of "S-k" becomes larger, the violation of voltage instead of the voltage stability issue, is more likely to happen.

Overload: Overloading conditions can also be a major abnormal phenomenon as a result of substation switching attacks. Once a heavily loaded line (or tie-line) between a large power station and load centers is disconnected, the power flow over the disconnected line is rerouted to the remaining available lines and those lines can be overloaded.

The stability limit may not necessarily be restricted by by the thermal limit and transient stability. The limit for frequency stability can restrain the power flow over the transmission line. In this case, such a transmission line has sufficient margin for the overloading before the switching attacks, and the possibility of the overloading due to substation switching attacks is unlikely. Transformers show a time-inverse characteristics for the overloading and some transformers have short-term and long-term limits. In sum, the combination of instability introduced can implicate the

overall control for destabilizing the grid.

4.1.3 Protective Relaying

Major protections are classified into: (1) line protection, (2) transformer protection, (3) bus protection, and (4) generator protection. It should be emphasized that the protections in transmission network are normally designed to detect the system faults with significant change in the voltage, current, and frequency to minimize the faulted section and to prevent power outages. Only when such significant change in electric quantities is observed/detected, the protections can initiate their actions. However, substation switching attacks do not always cause such a change in electric quantities. Therefore, protective relays that are designed for clearing the system faults are unlikely to operate in the case of substation switching attacks.

Line protection: Unlikely to operate except overloading protection

Bus protection: Unlikely to operate

Transformer protection: May operate over- or under- voltage protection

Generator protection: Likely to operate

4.1.4 Wide-Area Control and Protection

The local protection is designed to arm the grid avoiding equipment damage. On the contrary, the scheme of wide-area control and protection involves multiple substation coordination. Such schemes are categorized as:

- Protective relays to protect a component
- Protective relays to pre-empt the blackout.

The special protection system (SPS) is widely used to prevent cascaded events that cause the blackout. Although blackout are barely occurred [124], it is unevitable and its impact of blackouts is unignorable. The SPS is classified into two types: 1) response-based SPS, 2) event-based SPS [125, 126] (See Fig. 4.1 a)). The response-based SPS is provoked by detecting the dynamic behavior following a severe disturbance. Because remote or system-wide electric quantities are not generally required, this type has been typically implemented and used by utilities around the world. On the other hand, the event-based SPS normally requires system-wide information, but initiates the corrective action earlier than the response-based SPS, matching the event with the decision table As shown in Fig. 4.1 b), a fault detection function is often applied to activate the event-based SPS for higher reliability. The disruptive switching actions lead to the disconnection of the power equipment without any faults.

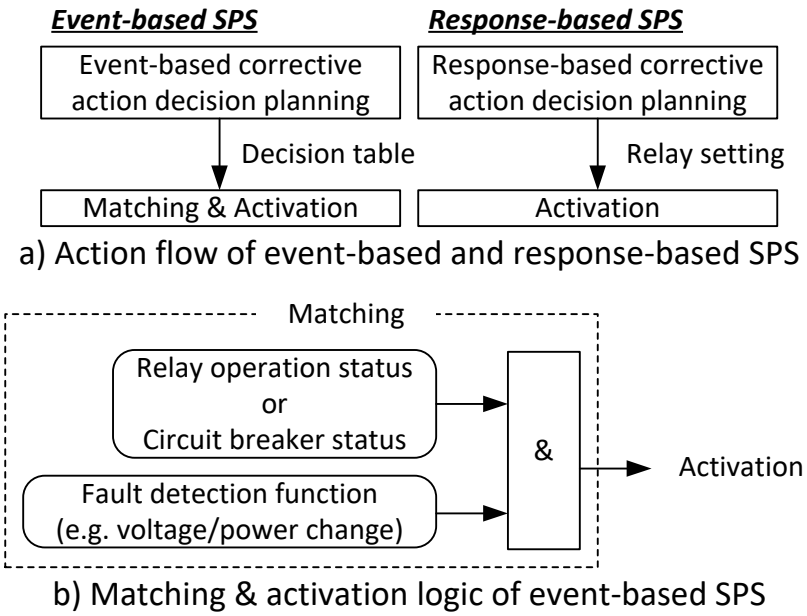


Figure 4.1: Event-based SPS and response-based SPS

Therefore, the event-based SPS do not initiate the corrective control action, while the response-based SPS can take that action. In light of this, the response-based SPS is out of scope of this simulation study.

4.1.5 Combinatorial Complexity for a Larger Power Grid

Statistically, an exhaustive enumeration of total substation outage combinations grows exponentially with the size of a power system [127]. The correlation is system-dependent where the the same size of the system under different topological setup would result in different combinations of diverged power solution solutions. The total numbers of substation in each power system could have different impact based on

the elimination methods at the lower k values, which is the number of substation outages. Efficient algorithms to include cascading outage and without outage have shown significant reduction of combination at the lower number of k; model with cascading outage would help to avoid large enumeration of evaluation with steady-state analysis [41, 42]. This chapter would adapt these algorithms to study combinations validating through dynamic simulation methods. On the other hand, complete enumeration without power system analysis tool can be computationally intensive [128] due to each combination would have to be validated to know if a scenario may lead to cascading blackout or brownout. An accurate assessment with time-domain analysis is needed in determining the significant impacts of the grid.

4.2 System Dynamics Under Switching Attacks

Cascaded events triggered by switching attacks from compromised substations hypothetically can be simulated in details using time-domain simulation tools [127]. If loads are connected to the compromised substation, those loads are manually disconnected by hackers and brownout can happen, the loss of electricity (LOE) is not zero. As k of S-k increases, the electricity loss caused by the manually disconnected power equipment is likely to increase because more substations are disconnected from the main grid. On the other hand, as k of S-k increases, the risk of additional disconnection caused by protective relays, *i.e.*, cascaded events, also increase. The risks

of cascaded events can lead to major brownout or blackout and a large number of protective relays operate before the power outage. Therefore, protective relays are modeled to capture the sequential dynamics in simulation where it captures cascade of grid instability.

However, protective relays for clearing short circuit faults or ground faults are unlikely to operate because fault currents are not created during substation switching attacks; meaning, protective relays that operate without fault currents are the pre-conditions of the grid before further analysis. In addition, the protective relays that operate *first* for the same power system dynamics (*i.e.* protective relays whose operating condition are more close to the normal operating condition), need to be properly modeled in the more realistic studies.

4.2.1 Frequency Relay

Frequency relay models are considered for synchronous generators, including synchronous condensers, and loads. The relay settings of overfrequency relays and underfrequency relays generally consist of a frequency level, a timer that impose delays and the undervoltage blocking function. The undervoltage blocking function disables tripping power equipment when the measured voltage is low, because the frequency relay fails to calculate the frequency accurately.

Because the frequency relay is often operated in multiple steps/stages, the multiple relay settings are often employed with the common undervoltage blocking function. In order to avoid the mechanical damage of the power plant, over speed protective relays are activated when the frequency significantly increases. However, over speed relays are unlikely to operate before the overfrequency relay operation because the frequency threshold level of over speed relays is higher than that of overfreuqency relays. Therefore, over speed relays may not kick in wake of the attack events.

4.2.2 Overvoltage Relay

Overvoltage relay models should be implemented for transformers and synchronous condensers, if any. The relay settings of overvoltage relays generally consist of a voltage level and a timer. Overvoltage relays may have the higher voltage level with the shorter timer, which is known as the instantaneous overvoltage relay.

4.2.3 Out-of-Step (OOS) Relay

Out-of-Step (OOS) relays [129] should be used for transmission lines as well as generators (including synchronous condensers, if any). OOS relay is designed using either the impedance or the voltage angle difference [116]. Although OOS relays are not

always placed in all of transmission lines in many countries, it is recommended to implement OOS relays to all of the lines for substation switching attack case studies from numerical stability point of view (Otherwise, the time-domain simulation can unexpectedly be terminated due to the numerical instability during cascaded events) as well as in the stability point of view.

4.2.4 Voltage/Frequency (V/F) Relay

The volts per hertz relay is generally implemented in generators. This relay can operate especially when the system frequency significantly goes down or when the terminal voltage significantly goes up. This protection may be skipped if overvoltage relay and underfrequency relay are modelled. Over-excitation limiters (OEL) [129] may be used on behalf of overvoltage relays because over-excitation limiters play a role to reduce the terminal voltage of generators. On the contrary, the OEL should be used if it is deployed in a generating unit.

4.2.5 Undervoltage Relay

Undervoltage relays should be used for loads. However, the typical relay settings of undervoltage relays are the threshold voltage level and its timer, and the typical

relay settings of the timer is 0.5 seconds or longer. On the other hand, the loads have their own disconnection characteristics in response to the voltage level and this self-disconnection characteristics reacts nearly instantaneously, *i.e.*, significantly faster than the operation of the undervoltage relay. Therefore, the modeling of the load self-disconnection characteristics is critical.

4.2.6 Automatic Voltage Controller

In order to represent the cascaded event more precisely, not only proper protective relay models, but also accurate generator models with controller models are vital. A representative exciter model should be implemented in generator models including synchronous condenser models. For the selection of the exciter model, the AC exciter is a general choice. In the case of the bulk power system with large capacity generators and poorly damped inter-area oscillations, the thyristor based exciter with the power system stabilizer (PSS) may be selected for a large capacity generator, such as 1 GVA class generators [130].

The aforementioned exciters must include over-exciter limiter (OEL) in modeling. This is due to the voltage imbalance can significantly change the filed voltage of generators can exceed its upper limit and the OEL starts to decrease the field voltage, which results in lower terminal voltage of the generator and lower reactive power

support from the generator. Although the response speed of the OEL is much slower compared to that of the AVR, the dynamic response of the OEL can shorten the time to blackouts especially when it takes longer time to result in blackouts. The generic model with its parameters is provided in references [131, 132].

4.2.7 Frequency Controller

The primary frequency model should be implemented into generator models excluding synchronous condenser models. Because most countries use thermal power unit as a major source, the simplified steam turbine governor model may be used as the generic power plant type. The generic model with its parameters is provided in references [132, 133].

The secondary and tertiary frequency controllers may be skipped for substation switching attack case studies mainly because the response time is not quite fast compared to the cascaded events after substation switching attacks. However, when the long-term stability study is required, the secondary frequency control, also known as automatic generation control (AGC) [129], should be considered in the modeling.

The power plant controller model [129, 133] that can precisely represent the dynamics of boiler and fuel controllers is suggested to be included especially when advanced

gasification combined power plants (AGCCs) [133] need to be modeled. The exhausted gas control reacts relatively fast and exhausted gas control can be prioritized depending on the ambient temperature and the active power output level. Generally speaking, the power plant controller model that represents modes of operations [129], either turbine-following mode or boiler-following mode, is critical and can significantly change the system frequency. However, there is currently no available generic power plant controller model with its parameters. Therefore, only when the real-life case study is performed and those information are available, that can be included in the modeling.

4.3 Modeling the System Specifics

The system diagram of the IEEE 14-bus system model is shown in Fig. 4.2. Ten substation locations are also shown using figures in a star box in the same figure. Fig.4.5 shows the power flow solution based on [46]. Because this system model is represented as of a part of American Electric Power System in 1962 [46, 130], the DC exciter model with the OEL is used as the exciter (see Fig. 4.3) and the primary frequency controller of steam turbines is used for both generators as the frequency controller of generators (see Fig. 4.4). Both units are assumed to be operated in regulated machines with the turbine output upper limit of 105% and the power plant controller and automatic generation control (AGC), *i.e.*, secondary frequency control

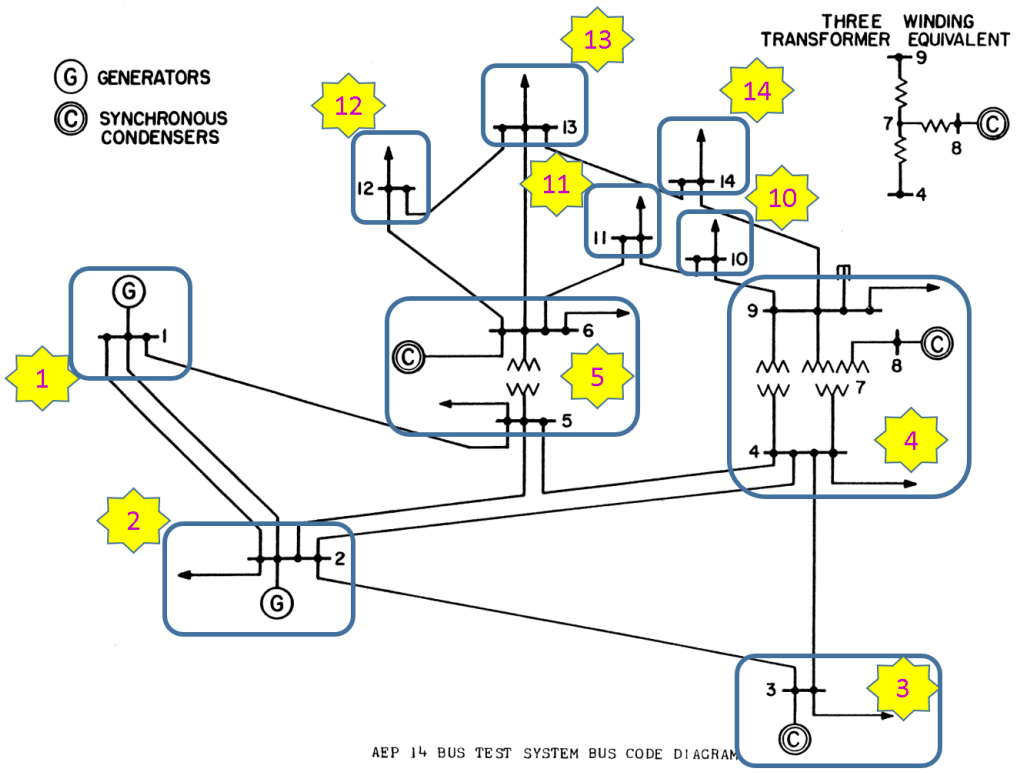


Figure 4.2: Single diagram of the IEEE 14 bus system model and assumed substation locations [21]

are not implemented in the model. It is noted that parameters shown in Figs. 4.3 and 4.4 are example parameters.

The rated capacity of a single thermal power unit in 1960s was less than 500 MVA, it is assumed that the Substation 1 includes three 100 MVA units with the output of 77.5 MW each. The assigned generator constants are shown in Table 4.1.

Table 4.1
Generator constants [134]

Specification	G1			G2
	G1-1	G1-2	G1-3	
Rated Capacity [MVA]	100	100	100	60
Rated Power [MW]	85	85	85	51
Inertia Constant, M [s]	6	6	6	6
D-axis Reactance [p.u.]	1.7	1.7	1.7	1.7
D-axis Transient Reactance [p.u.]	0.35	0.35	0.35	0.35
D-axis Sub-transient Reactance [p.u.]	0.25	0.25	0.25	0.25
Q-axis Reactance [p.u.]	1.7	1.7	1.7	1.7
Q-axis Sub-transient Reactance [p.u.]	0.25	0.25	0.25	0.25
D-axis Transient Time Constant [s]	1	1	1	1
D-axis Sub-transient Time Constant [s]	0.03	0.03	0.03	0.03
Q-axis Open Circuit Time Constant [s]	0.206	0.206	0.206	0.206
Q-axis Sub-transient Time Constant [s]	0.03	0.03	0.03	0.03
Armature Leakage Reactance [p.u.]	0.225	0.225	0.225	0.225
Armature Time Constant [s]	0.4	0.4	0.4	0.4
Zero Phase Reactance [p.u.]	1.7	1.7	1.7	1.7
Negative Phase Reactance [p.u.]	0.25	0.25	0.25	0.25

4.3.1 Modeling the Frequency Deviation in Relays

The following settings of overfrequency and underfrequency relays for generators (including synchronous condensers) are as follows: [135, 136].

- 61.8 Hz (overfrequency relay)
- 58.0 Hz (underfrequency relay)

Example relay settings of underfrequency relays for loads are in the following [135,

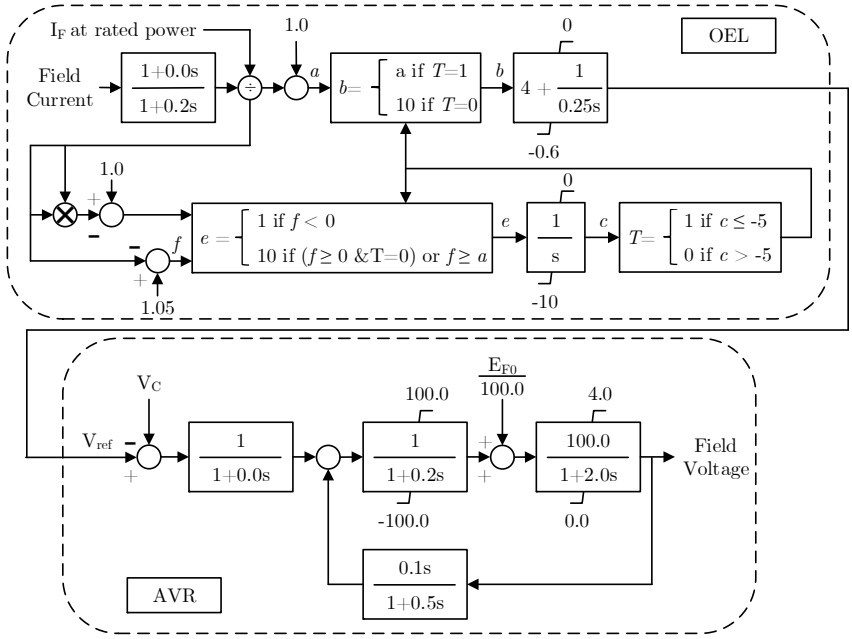


Figure 4.3: AVR model with OEL model [134]

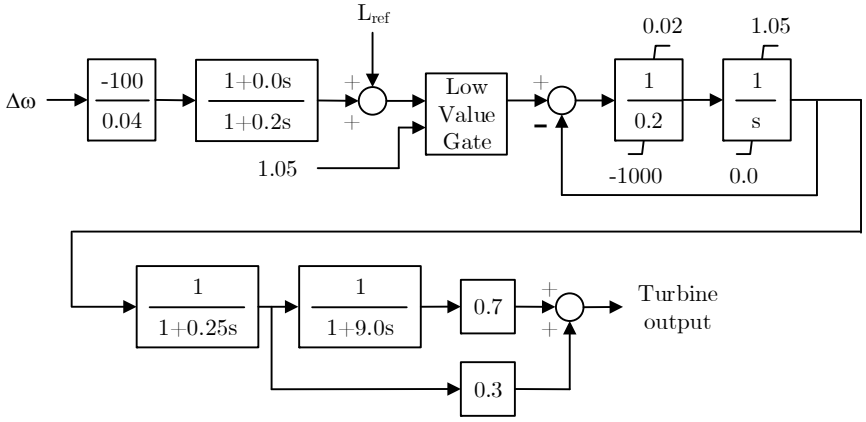
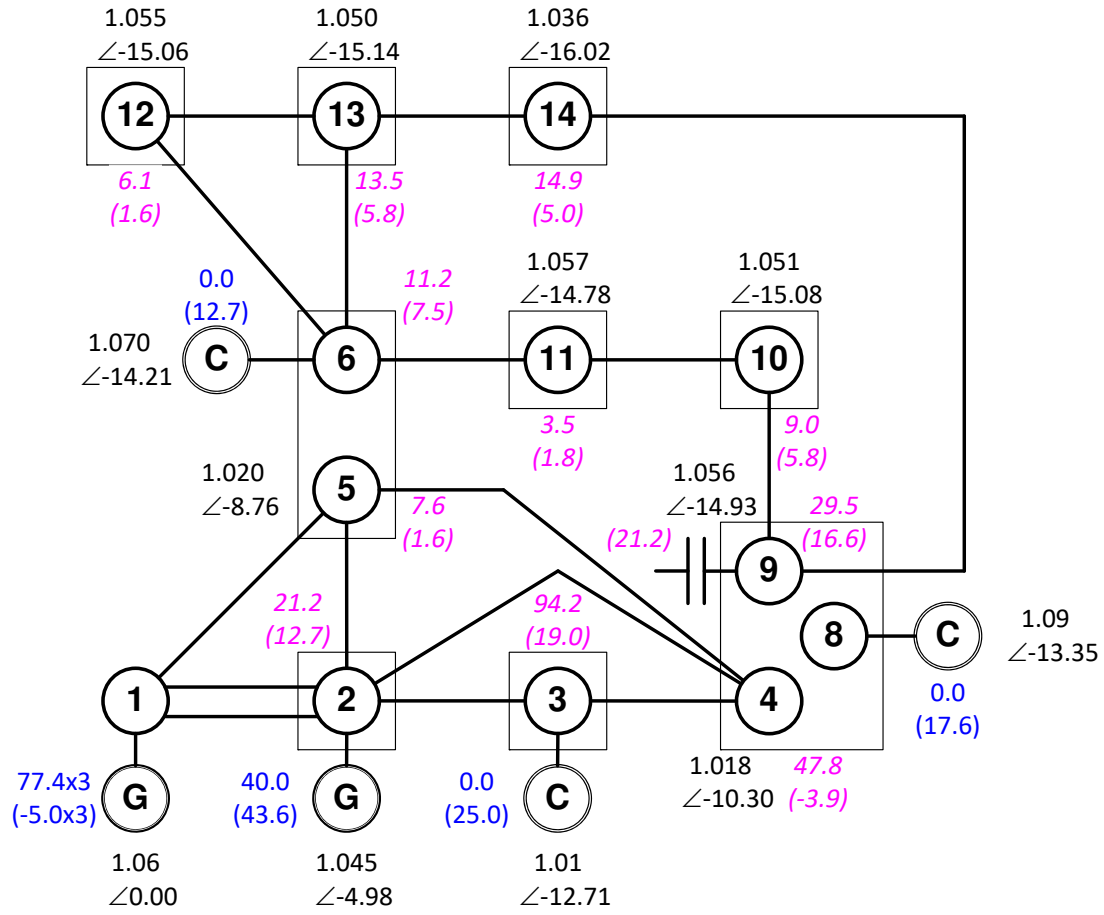


Figure 4.4: Primary Frequency Control model [134]

136].

- 59.3 Hz (5% reduction with relative to the total load)
- 58.9 Hz (additional 10% reduction with relative to the total load)
- 58.5 Hz (additional 10% reduction with relative to the total load)



Blue: Active power output of generator [MW] (Reactive power output [Mvar])

Pink: Active power load consumption [MW] (Reactive power load consumption [Mvar])

Black: Magnitude of bus voltage [p.u.] with angle of bus voltage [degrees]

Figure 4.5: A Power flow solution using IEEE 14-bus system model

Note that the maximum load shedding amount is of 25% for the total loads. Because the undervoltage locking level is often set as 0.4 p.u., the value is then used, which means the frequency relay does not trip the loads when the voltage level is under 40%. The other parameters include timer is set to zero in the case studies, while the circuit breaker operation time is set as 70 ms.

4.3.2 Overvoltage Relaying

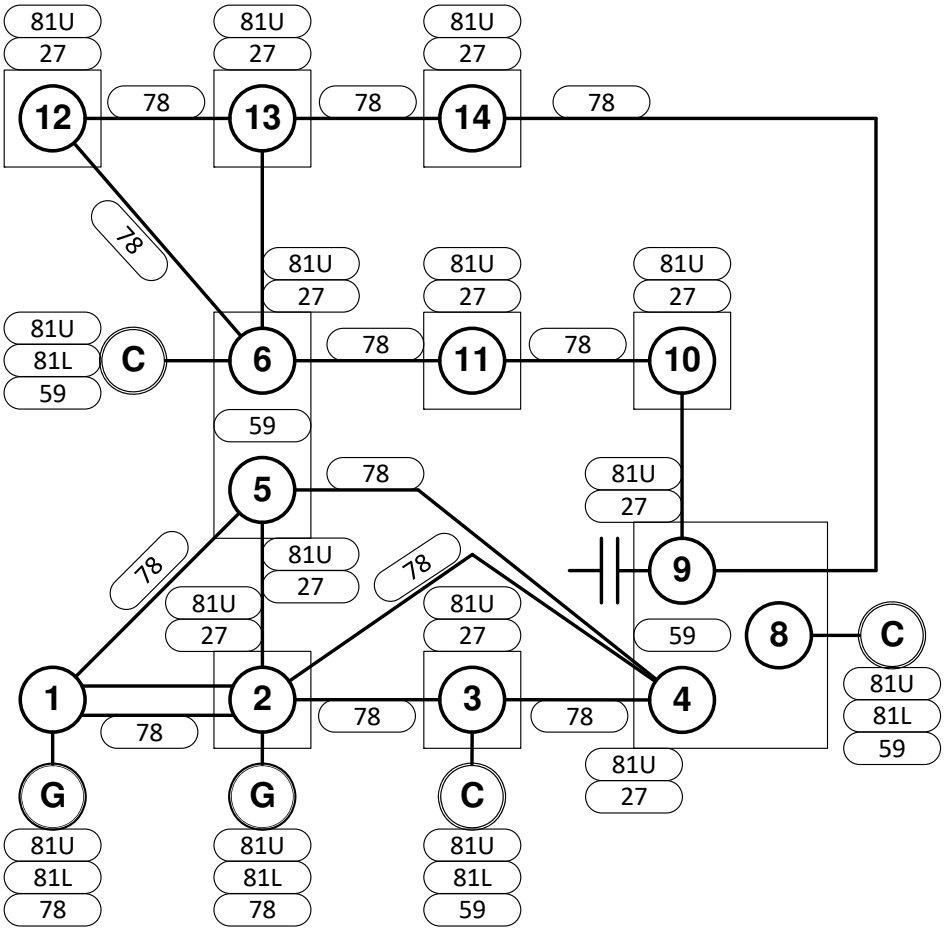
The following parameters of overvoltage relays are implemented in [137],[138]:

- 115% (Overvoltage relay with time=1s)
- 125% (instantaneous overvoltage relay with time=30ms)

In addition to the timer imposed, the circuit breaker operation time is set as 70ms.

4.3.3 Out-of-Step Blocking

The voltage angle difference between the terminal voltage and the internal induced voltage is used for the Out-Of-Step (OOS) relay for synchronous generators, while the voltage angle difference between transmission lines is use for the OOS relay for networks. When the voltage angle difference is used for OOS relays, the relay setting is set as 180 degrees between the two buses according to the definition of the OOS condition. Although the timer is set as zero, the circuit breaker operation time is set as 30 ms. A typical setup of relaying combination for each substation is illustrated in Fig. 4.6. This setup is used for simulation of switching attack simulation.



81U: Overfrequency relay

81L: Underfrequency relay

78: Out-of-step relay

59: Overvoltage relay

27: Underfrequency relay emulated by load self-disconnection characteristics

Note: The assigned numbers are based on [139].

Figure 4.6: Deployment of relay models in IEEE14-bus system model [134]

4.3.4 Modeling the Electrical Loads

Load characteristics are represented using the exponential load model with the voltage and frequency dependent as shown in Eq. (4.1) [129, 140]. Load voltage characteristics indices are based on widely used parameters for power system analysis in utilities and system operators [141]. The coefficients of Load frequency characteristics are set based on the International Council on Large Electric Systems (CIGRE) working group which goes through substantial studies on the utility's grid systems from around the world [142].

$$P = P_0 \left(\frac{V}{V_0}\right)^1 \left(1 + \frac{3.33}{100}\Delta f\right) = P_0 \left(\frac{V}{V_0}\right) \left(1 + \frac{3.33}{100}\Delta f\right) \quad (4.1)$$

$$Q = Q_0 \left(\frac{V}{V_0}\right)^2 \left(1 + \frac{0}{100}\Delta f\right) = Q_0 \left(\frac{V}{V_0}\right)^2 \quad (4.2)$$

where,

P_0**:** Initial active power consumption of loads

Q_0**:** Initial active power consumption of loads

V_0**:** Initial load bus voltage

P**:** Active power consumption of loads

Q**:** Reactive power consumption of loads

V**:** Load bus voltage

Δf**:** Frequency deviation [Hz]

The loads defined here is an aggregated electricity consumption of thousands of consumers at high voltage transmission network. The aggregated loads in distribution network [143] represents a fraction of high voltage loads. The modeling of loads is an empirical study that accumulates the statistical correlation between voltage and current magnitudes from the current and potential transformers (CT/PT).

4.3.5 Undervoltage Phenomena and Load shedding Scheme

The load self-disconnection characteristics are summarized in the following [144]:

Load Self-disconnection Voltage: Below 80%

Load Self-disconnection Starting Voltage: 80%

Load Self-disconnection Saturation Voltage: 40%

Maximum load Self-disconnection Amount: 25%

This characteristic illustrated in Fig. 4.7 are employed by all loads (both active power loads and reactive power loads) and superimposed on the load voltage and frequency characteristics shown in Equation 4.1. Because disconnected loads do not

normally recover quickly and it takes over a minute for many loads to recover, load recovery characteristics are not considered in the model. For example, once the load bus voltage level is below 40% under the rated frequency, 25% of the loads are disconnected, and the remaining 75% loads that stay connected reduce the active and reactive power consumption to 40% and 16% (=0.4^2), individually, due to the load voltage characteristics. The following case studies are performed using a commercially available time-domain simulation tool [145].

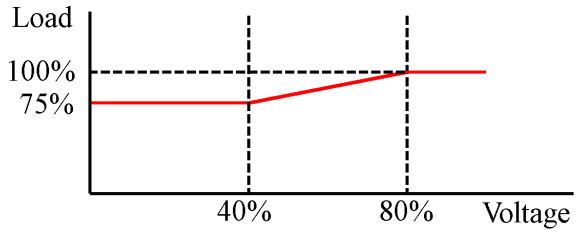


Figure 4.7: Load self-disconnection model [134]

4.4 Event Replay with Cascaded Relay Resulting in Power Outage

4.4.1 Case 1: Sequence of Relay Operation

The sequential relays are initiated by the switching attack on substations 2 and 12 in Fig. 4.2 where it is referred to one combination of S-2 cases. This serves as the

initiating events where assumptions made here is that attackers successfully hack into the substation through the substation firewall and have compromised the substation console that has accessed to all substation breakers.

As shown in Fig. 4.8, protective relays at different locations are operated sequentially during the cascaded stage. As shown in Fig. 4.9, the underfrequency relay operations for load at 0.06s through 0.36s are aggregated. In this example substation switching attack, one of the generators is isolated due to the attack and tripped 0.3s after the switching attack due to the overfrequency relay operation. The protective relay operation for the isolated component is not included in Fig. 4.9.

In this study case, the synchronous generator at Bus 1 is accelerated after the switching attack, while the synchronous condensers is decelerated after the switching attack. This discrepancy comes from the opposite magnitude relation between the mechanical output and electrical output of those synchronous machines.

The output of synchronous condensers is zero at the steady state. However, it immediately increases using its rotating energy, *i.e.*, the inertia shown during the occurrence of attack at substations 2 and 12. Because the electrical output is larger than the mechanical output for that time period, the rotating speed of synchronous condensers decreases, which is indicated by the measured frequency decrease.

On the other hand, the electrical output of the synchronous generator at Bus 2

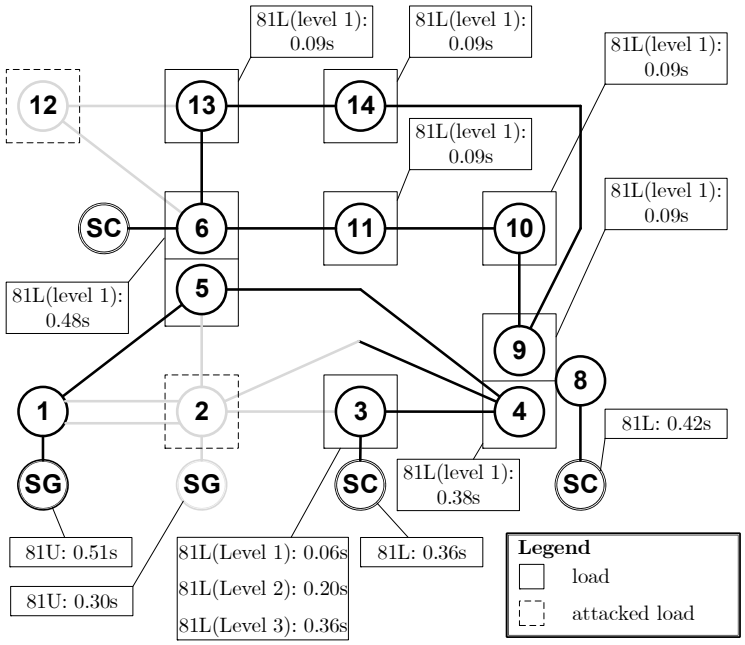


Figure 4.8: Relay operation time for substation switching attack on Substations 2 and 12 [134]

decreases when the attack at substations 2 and 12 occurs because the deficiency of the active power output is compensated by synchronous condensers as well as the synchronous generator at Bus 2. Therefore, the electrical output is smaller than the mechanical output following the substation switching attack, the rotating speed of synchronous generator at Bus 1 increases, *i.e.*, the measured frequency increases.

Therefore, the underfrequency relays for the loads and synchronous condensers operate, while the overfrequnecy relay for the synchronous generator at Bus 1 operates at 0.51s, which results in the blackout.

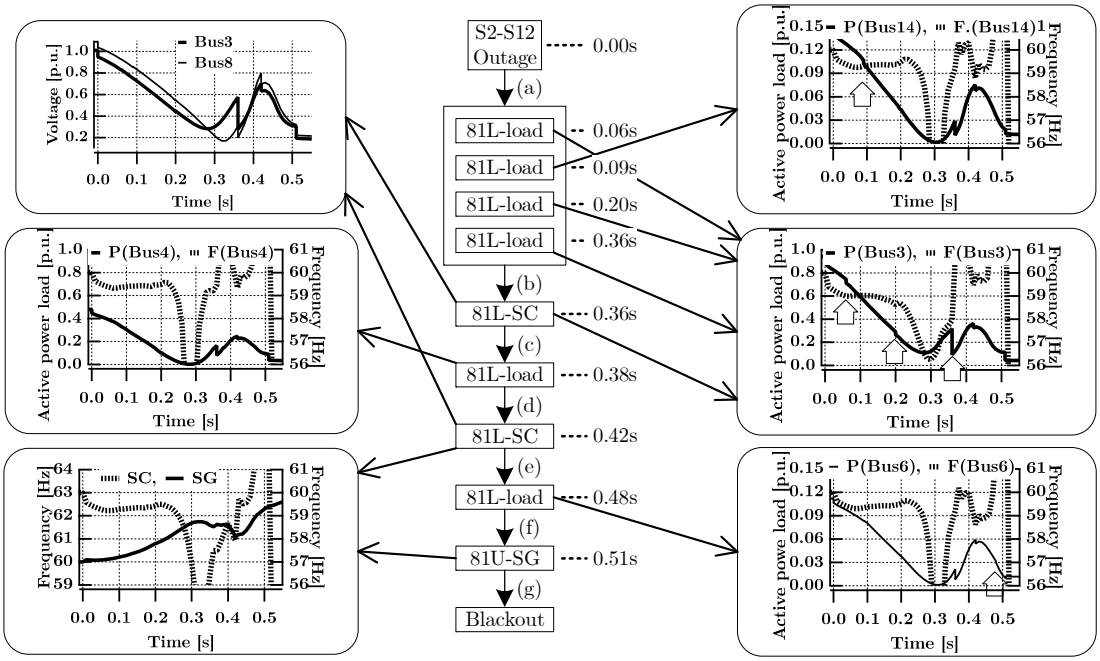


Figure 4.9: Sequence of relay operation with corresponding waveform [134]

4.4.2 Case 2: Sequence of Relay Operation

The sequential relays are initiated by the switching attack on substations 1, 3, 10, 11, 12, 13, and 14 in Fig. 4.10 where it is referred to combinations of S-7 cases. Protective relays at different locations including overvoltage relays are operated sequentially during the cascaded stage. As shown in Fig. 4.11, the underfrequency relay operations for load at 0.05s through 0.15s are aggregated. In this example substation switching attack, one of the generators is isolated due to the switching attack and tripped 0.24s after the switching attack due to the overfrequency relay operation. The protective relay operation for the isolated component due to the switching attack is not shown in Figs. 4.10 and 4.11.

In this study case, the synchronous generator at Bus 2 is decelerated after the switching attack, while the disconnected synchronous generator at Bus 1 is accelerated after that. As shown in Fig. 4.12, the electric power output at Bus 2 increased immediately right after the switching attack. Because the electric output exceeds the mechanical input of the generator at Bus 2, the rotating speed of the generator starts to decrease, which results in decrease in the system frequency.

On the other hand, the terminal voltage of synchronous condensers at buses 6 and 8 increased by over 10% and reach to over 115% right after the switching attack. Synchronous condensers generally contribute to increase the system voltage providing reactive power at heavily load conditions. Before the substation switching attack, the synchronous condensers at buses 6 and 8 are connected to the medium point of the grid between power stations and loads. However, after the substation switching attack, those condensers are eventually connected to the end of the grid as shown in Fig. 4.12, losing the supporting loads, and their terminal voltages are raised.

As the system frequency decreases, the connected loads are gradually disconnected due to underfrequency relays, which leads to lighter loading condition, and the system voltage further increases and reaches to over 125%. Therefore, instantaneous overvoltage relays of one synchronous condenser at bus 6 and transformers near bus 6 at 0.19s. It is noted that undervoltage relay operation at bus 6 in Figs. 4.11 and 4.12

is the results of disconnection of the transformer at bus 6, not the reason of the substation switching attack. After disconnecting them, the system voltage additionally increases and the rest synchronous condenser and the transformer are disconnected due to the overvoltage relay at 0.20s, which is a typical cascading event.

The immediate increase in the system voltage at 0.20s contributes to increase the total demand due to the load voltage characteristics, which accelerates the decrease in the system frequency and trip the remaining generator at bus 2 due to the underfrequency relay at 0.21s. It is noted that undervoltage relay operations at buses 2, 4, and 9 in Figs. 4.11 and 4.12 are the results of the blackout, not the reason of the blackout. Therefore, the underfrequency relays for the loads and synchronous condensers operate, while the overfrequnecy relay for the synchronous generator at Bus 1 operates at 0.51s, which results in the blackout.

4.4.3 Case 3: Sequence of Relay Operation

The sequential relays are initiated by the switching attack on substations 2, 10, and 11 in Fig. 4.13 where it is referred to one combination of S-3 cases. Protective relays including OOS protections at different locations are operated sequentially during the cascaded stage. Fig. 4.14 illustrates the underfrequency relay operations for load between 0.06s and 0.24s may be aggregated. In this example substation switching

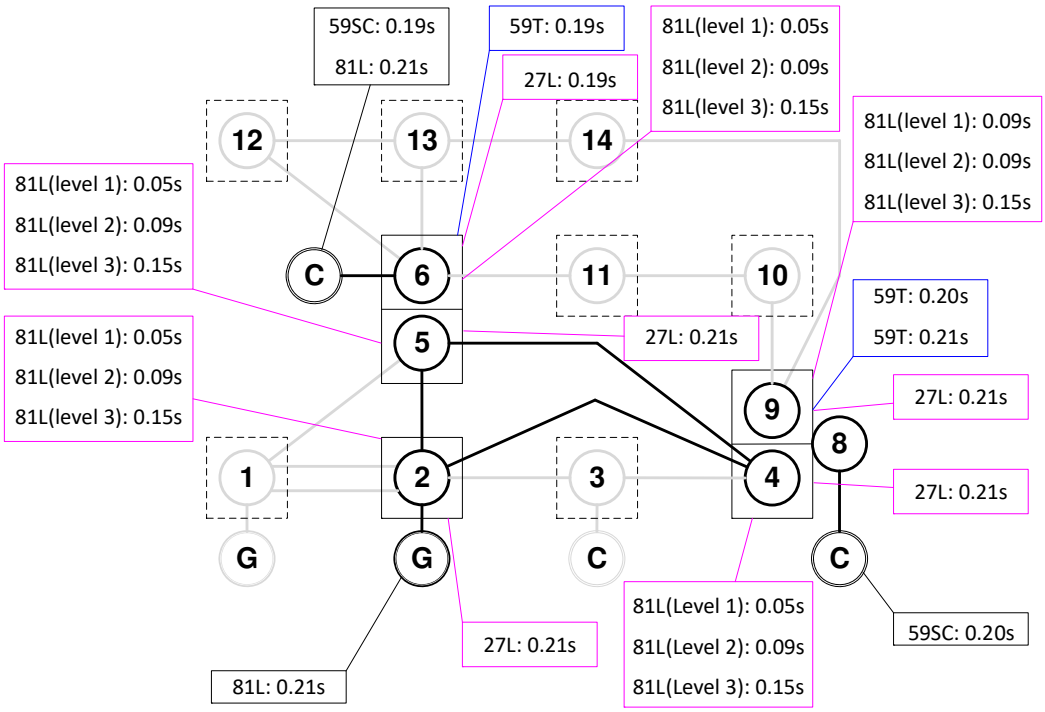


Figure 4.10: Sequence of relay operation [134]

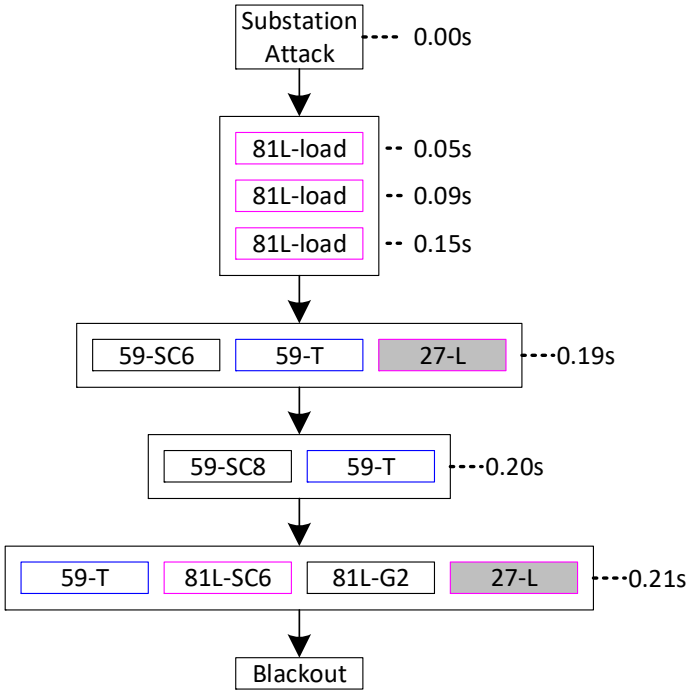


Figure 4.11: Sequence of relay operation [134]

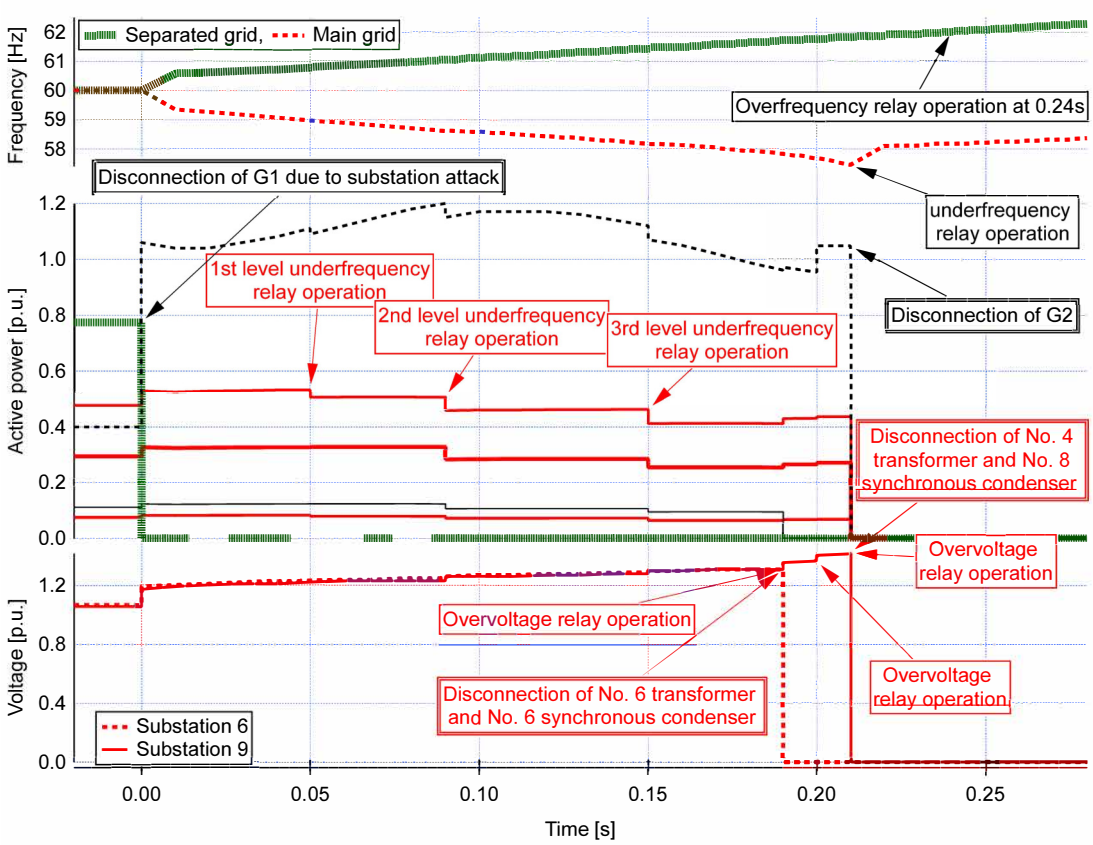


Figure 4.12: Phenomenon of system dynamics for the IEEE 14-bus system [46] initiated by a substation switching attack upon substation 7 [134]

attack, one of the generators at bus 2 is isolated due to the switching attack and tripped 0.30s after the switching attack due to the overfrequency relay operation.

Referred to Clause 4.4.1, the connecting synchronous generator at bus 1 is accelerated while synchronous condensers decelerate. In this case, as the discrepancy of the rotor speed between the synchronous generator and the synchronous condensers increases, (the twist of) the angle difference between them also increases, which results in the out-of-step conditions at two locations (over the line between buses 4 and 5 and the line between buses 6 and 12) at 0.33s and 0.34s. After the loss of two lines,

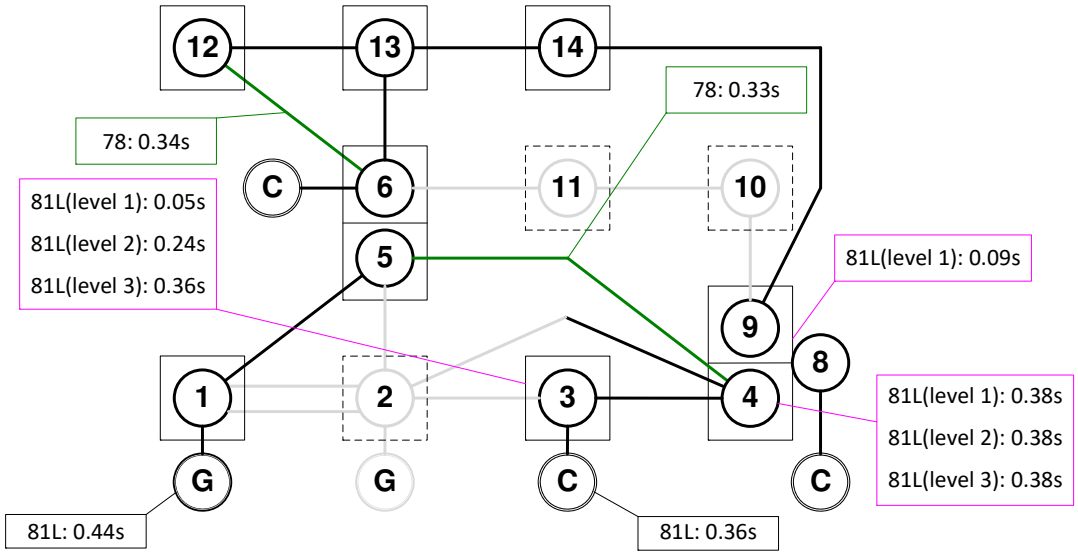


Figure 4.13: Sequence of relay operation [134]

the electrical distance between the source and loads is expanded, and the remaining generator at bus 1 is tripped by overfrequency relay.

4.4.4 Losses of Electricity

The losses of electricity (LOE) are often considered the pre-cursor of grid instability. Statistically, the following simulated statistics of LOE for the case study in IEEE 14-bus system is shown below:

0 $\sim$ 9.99%: 21 cases

10 $\sim$ 19.99%: 30 cases

20 $\sim$ 29.99%: 12 cases

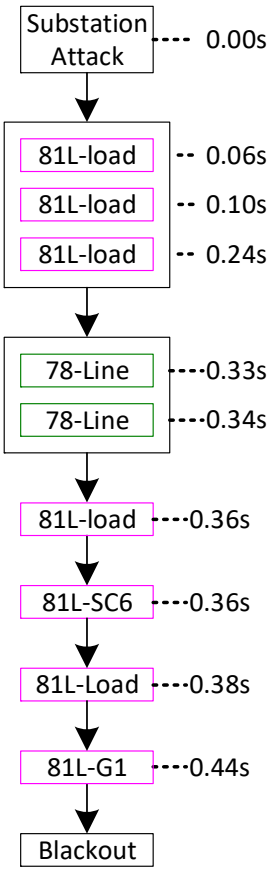


Figure 4.14: Sequence of relay operation initiated by tripping substations [134]

30 ∼ 39.99%: 30 cases

40 ∼ 49.99%: 2 cases

50 ∼ 59.99%: 0 cases

60 ∼ 69.99%: 0 cases

70 ∼ 79.99%: 0 cases

80 ∼ 89.99%: 8 cases

90 ∼ 99.99%: 0 cases

100%: 950 cases

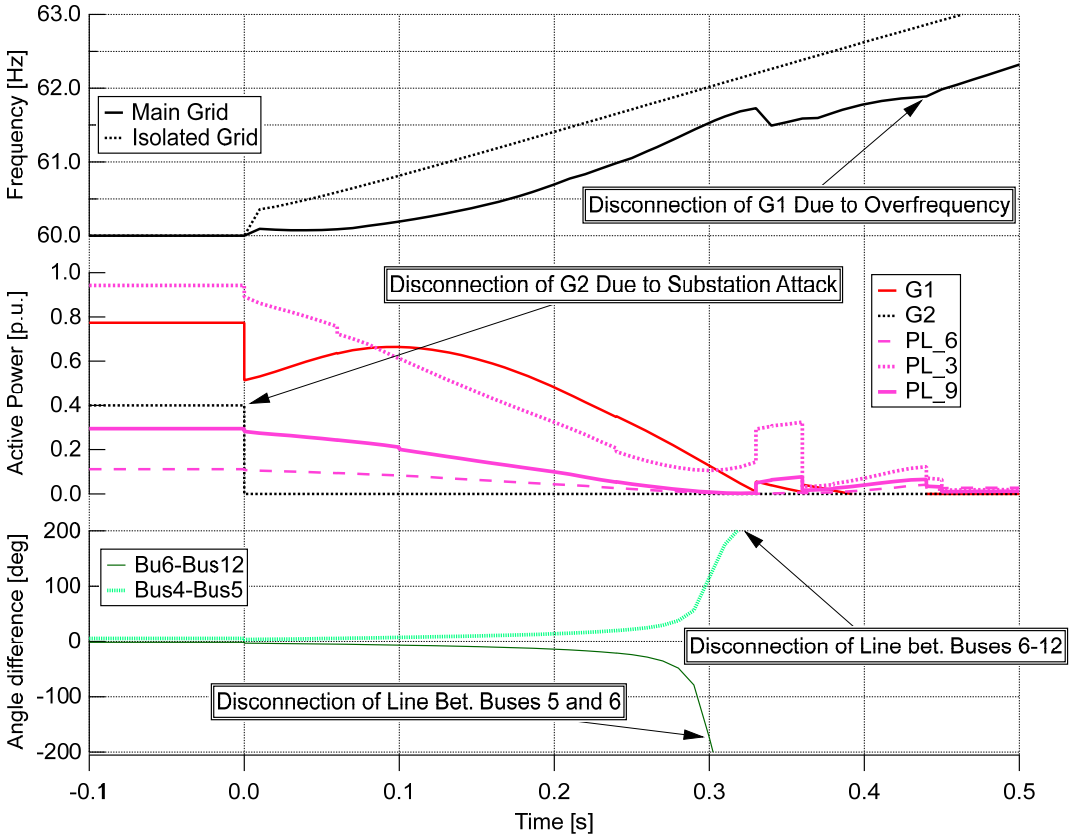


Figure 4.15: Phenomenon of system dynamics for the IEEE 14-bus system [46] initiated by a substation switching attack upon substations 2, 10, and 11 [134]

Under this study of simulation, the percentage of evident number of blackouts for k from 1 to 10 of S-k has reached 92.3%. The simulation results have shown that the original hypothesis of assumption, which is the total combinations of blackout cases decrease as the size of the grid is larger for $k \leq 10$. The constant 10 is arbitrarily assigned based on the knowledge of simulation study that optimally provides the intuition of study that shows the cutoff of large combinations for the first 10 order.

4.5 Extensive Cyber-Based Contingencies

4.5.1 S-k Contingency

This is a classical study of cyber-based contingency under steady-state analysis. The presumed outages of components associated with each node of transmission network (referred to substation outages) is removed from the base cases. However, such studies do not include sequential events in "time" to demonstrate the cascading [146] and it can be challenging to capture blackout/brownout in steady-state simulation. The "divergence" of power flow solutions is the only indicator to show that system reaches its limit and such simulation study can be pre-screening. Investigation of dynamic study may exhibit the scenarios otherwise, depending on the relay models that capture the cascades. This approach is improved computationally by eliminating the combinations in the early stage of k so that a larger number of combinations would not carry forward to the higher number of k. Such approach can significantly reduce total combination when incorporated the cascading effect using power flow method (steady-state). The advantage of this approach can stimulate the combinatorial cases in a shorter time using practically-sized transmission network that can be very useful for simulating a studied network for actuarial science that can be quantitatively utilized to estimate risks.

4.5.2 R-k Contingency

Each substation is gradually replaced with digital relays for modernization of IP-based substations. Depending on the relay types, each relay is connected to different part of the circuit breakers in a substation. While this may prove the usefulness of details in term of impacts, the types of deployed relays in a power system can be complex to mimic the real scenarios. This sort of contingency can be structured between S-k and N-k/N-1 [147]. Without systematic elimination techniques, it can be computationally challenging for each base case, especially when the size of a power system is larger than 1000-bus system. This framework is under development.

4.6 Impact Evaluation

A hypothesized impact study evaluates the plausible consequence of cyberattacks and anticipates system behaviors based on a specific operating condition. Such prediction of potential cascading outages and failures can be utilized to derive metrics that quantify the attributes of a case study. This requires validation of impact credibility on methods used in steady-state and dynamic simulations. A conceptualization of impact evaluation is proposed to handle the combinatorial nature of cyber-related issues associated with :

- Critical/non-critical combination verifications,
- Cascade confirmation,
- Re-evaluation.

4.6.1 Critical/Non-Critical Combination Verifications

This verification involves a steady-state and dynamic analysis of the hypothesized components and substation outages. This checkpoint is used to determine inconsistent simulation outcomes from both dynamic and static modules and reconcile the difference through cascade confirmation and probability re-evaluation through an adjustment of parameters. For example, a hypothesized substation outage would result in power flow diverged that may not necessarily reflect a similar dynamic simulation outcome. This could happen when a power flow simulator shows no cascading failure symptom, but the dynamic study indicates otherwise.

4.6.2 Cascade Confirmation

The cascade confirmation proposed here is to determine the coherency of relative angle and frequency under specific switching permutation. The studies will include determining the number of permutations deemed conclusive and adequate, corresponding to sequential contingencies. The effective pre-screening of sequential contingencies

would include substation dependencies and the practicality of concurrent cyberattacks to disconnect components/substations out of the grid abruptly. The challenges here adequately represent an unordered combination of outage from the steady-state power flow module.

4.6.3 Re-Evaluation

Re-evaluation often occurs when both simulators demonstrate a significant deviation of outcome that requires an adjustment. Such errors can be related to either of the simulators where specific handling is necessary. The discovery of tuning between the two modules can significantly reduce the discrepancies and will strengthen the verification and credibility of the hypothesized scenarios. The results depend on the size of a power system. Fig. 4.16 enumerates all critical and non-critical cases and illustrates cascaded evaluation with steady-state rapid screening to dynamic simulation to verify the catastrophic scenarios. The divergence evaluation in a power flow model determines the criticality of hypothesized substation outages. However, the steady-state evaluation results may not consistently demonstrate the same outcome in the sense of potential grid instability of cascading implication. Fig. 4.16 describes the dependencies of steady-state simulation screening with a probability of the critical contingency P that is derived as 0.1%, while the probability of the non-critical contingency is derived as 99.9%. The summation of probabilities at each level (steady-state

and dynamics) is always equal to 1.0. These probabilities are the statistical numbers established to determine the total number of convergent and divergent cases. The steady-state approach would largely eliminate the criticality of problematic scenarios, which may not always be correct. The latter part of the dynamic simulation examines the consistencies of both methods, whether they are stable or unstable from the power system stability point of view. This may not always be the same between both. The verification of dynamic simulation could reveal the criticality of non-critical contingency, which is statistically derived. As shown in the figure, the critical combinations with probability 0.1% based on steady-state simulation will be examined with the dynamic simulation that may result in 73.5%. On the other hand, the dynamic simulation verification can also reveal the probability of the critical contingency that is statistically derived by 4.7% from the steady-state probability of the non-critical contingency, which is 99.9% in most cases. Computationally, the steady-state approach is much less expensive than the dynamic simulation verification, while the latter approach has a higher degree of accuracy with a detailed description of system behaviors.

In general, steady-state analysis may not always reflect a potential issue of potential cascading, especially the transient states are not sequentially captured one after another subsequent outages. The stability evaluation of cascading outages is a dynamic-security analysis with variables in transient status such as time period, frequency and voltages instability, generation-load imbalance, and metrics of cost-benefit

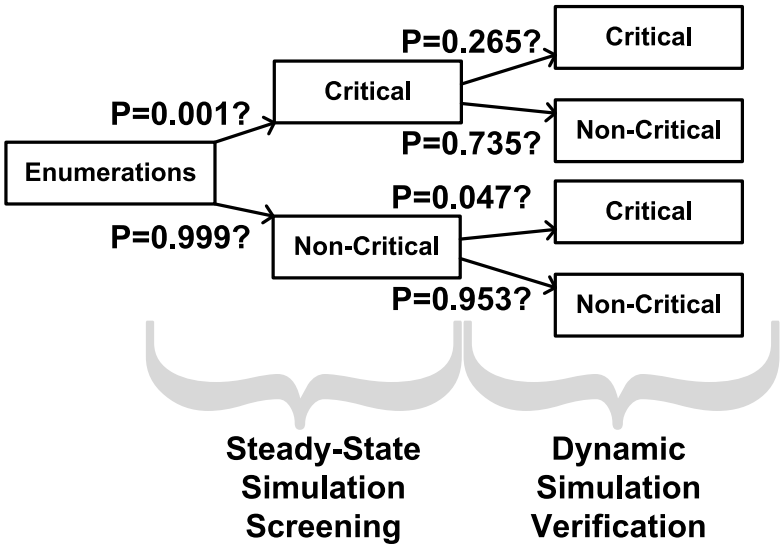


Figure 4.16: Enumerative grouping for critical and non-critical cases [127]

justification of catastrophic impacts [146, 148, 149, 150]. For example, the mismatch of generation and load in power flow evaluation model can be numerically balanced on the "reference" node, where physically, there is no slack bus in the practical world. The imbalance of generation and load can only be achieved by adjusting generation output and/or shedding load. The time transition of one state to another is not sequentially captured in the steady-state power flow model – the power flow evaluation solely addresses the divergence-convergence issue which is directly related to the initiation of voltage, generation, bus type, and topology of power system. The time interval is critical in the dynamic analysis with cascading outages. Sequential cascading events can be induced in a bulk power system after an initial cyberattack that can range in an interval of 5s to 15s for a switching action initiated by attacker

automation tools. The operation condition of power system should reflect the transition states that may lead to unstable or not in term of generator ramping up/down or load shedding as well as the influence of various protection scheme deployed on any microprocessor-based components within a substation-level network. Consequently, the active power flow of each transmission line needs to be updated during each time interval. Moreover, under certain circumstance, the models of steady-state analysis may be inadequate to detail the sequential disruptive switching permutation under a substation specific scheme, e.g., one-an-half bus-breaker model because the IEEE test case may be simplified in most of the steady-state analysis appeared in the literature. The accuracy of dynamics simulation may necessarily needs a more detailed topology for such study. Additionally, the steady-state analysis may not be able to capture islanding issue when a cascading outage occurs [151, 152]. In a larger system, the initiating event of switching attacks upon the substations may initiate a breaker tripping that results in multiple islands. This can be a unique situation where power flow verification may not always agree with a diverged outcome if multiple islands are discovered and the handling of multiple "slack" buses may not immediately compensate the generation-load imbalance across the islands. Without a methodological approach, there may not be a direct way to conclude that stabilities can be achieved among these multiple islands as a result of a cyberattack initially.

4.7 Simulation Results for S-k Contingency

4.7.1 Power Flow Based Blackout Rate

The brownout rate and blackout rate in the IEEE standard systems are derived from a power flow calculation program.

4.7.1.1 IEEE 14-bus system

The blackout rate rapidly increases as k of S-k increases while k is below 5 in the IEEE 14-bus system (Table 4.2). When k is equal to or more than 5, the increase in the blackout rate is saturated in the IEEE 14-bus system. k of over 8 of S-k is skipped because blackout rate is always one. It is noted that the IEEE 14-bus system comprises 10 substations.

4.7.1.2 IEEE 30-bus system

The blackout rate rapidly increases as k of S-k increases while k is below 6 in the IEEE 30-bus system (Table 4.3). When k is equal to or more than 6, the increase in the blackout rate is saturated in the IEEE 30-bus system. k of over 11 of S-k is

Table 4.2
Power flow based brownout and blackout cases of S-k contingency analysis using IEEE 14-bus system

S-k	Brownout (convergence)	Blackout (divergence)	Blackout rate
S-1	7	3	0.400
S-2	20	25	0.667
S-3	30	90	0.833
S-4	25	185	0.929
S-5	11	241	0.964
S-6	2	208	0.971
S-7	0	120	0.983
S-8	0	45	1.000

skipped because blackout rate is always one. It is noted that the IEEE 30-bus system comprises 24 substations.

Table 4.3
Power flow based brownout and blackout cases of S-k contingency analysis using IEEE 30-bus system

S-k	Brownout (convergence)	Blackout (divergence)	Blackout rate
S-1	20	8	0.286
S-2	115	161	0.583
S-3	478	1,546	0.764
S-4	1,255	9,371	0.882
S-5	2,143	40,361	0.950
S-6	2,348	132,248	0.983
S-7	1,618	344,486	0.995
S-8	678	734,793	0.999
S-9	156	1,307,348	1.000
S-10	15	1,961,241	1.000
S-11	0	2,496,144	1.000

4.7.1.3 IEEE 57-bus system

The blackout rate rapidly increases as k of S-k increases while k is below 6 in the IEEE 57-bus system (Table 4.4). When k is equal to or more than 6, the increase in the blackout rate is saturated in the IEEE 57-bus system. k of over 19 of S-k is skipped because blackout rate is always one.

Table 4.4
Power flow based brownout and blackout cases of S-k contingency analysis using IEEE 57-bus system

S-k	Brownout (convergence)	Blackout (divergence)	Blackout rate
S-1	25	17	0.405
S-2	293	568	0.660
S-3	2,134	9,346	0.814
S-4	10,807	101,123	0.903
S-5	40,343	810,325	0.953
S-6	114,826	5,130,960	0.978
S-7	254,324	26,724,004	0.991
S-8	443,899	117,586,286	0.996
S-9	615,204	445,276,606	0.999
S-10	679,422	1,470,763,551	1.000
S-11	597,624	4,279,963,752	1.000
S-12	416,539	11,057,700,349	1.000
S-13	227,579	25,518,503,701	1.000
S-14	95,659	52,860,133,421	1.000
S-15	29,964	98,672,397,652	1.000
S-16	6,607	1.66510E+11	1.000
S-17	916	2.54662E+11	1.000
S-18	60	3.53697E+11	1.000
S-19	0	4.46775E+11	1.000

4.7.1.4 IEEE 118-bus system

The blackout rate rapidly increases as k of S-k increases while k is below 6 in the IEEE 118-bus system (Table 4.5). When k is equal to or more than 6, the increase in the blackout rate is saturated in the IEEE 118-bus system. k of over 7 of S-k is not calculated because extremely large arrays needs to be allocated and the memory error derails the calculation.

Table 4.5
Power flow based brownout and blackout cases of S-k contingency analysis using IEEE 118-bus system

S-k	Brownout (convergence)	Blackout (divergence)	Blackout rate
S-1	67	42	0.385
S-2	2,167	3,719	0.632
S-3	45,107	164,827	0.785
S-4	666,054	4,897,197	0.880
S-5	7,503,993	109,324,278	0.936
S-6	66,795,314	1,958,228,050	0.967
S-7	483,308,071	29,313,464,285	0.984

4.7.2 Dynamic Simulation Based Blackout Rate

The brownout rate and blackout rate in the IEEE standard systems are derived from a commercially available time-domain simulation tool [145].

4.7.2.1 IEEE 14-bus system

The blackout rate rapidly increases as k of S-k increases while k is below 5 in the IEEE 14-bus system (Table 4.6). When k is equal to or more than 5, the increase in the blackout rate is saturated in the IEEE 14-bus system. If k is over 7, any cases incur blackouts. The S-10 is skipped because it is obvious that the grid results in the blackout.

Table 4.6
Dynamic simulation-based brownout and blackout cases of S-k contingency analysis using IEEE 14-bus system

S-k	Brownout (stable)	Blackout (unstable)	Blackout rate
S-1	6	4	0.400
S-2	15	30	0.667
S-3	20	100	0.833
S-4	15	195	0.929
S-5	9	243	0.964
S-6	6	204	0.971
S-7	2	118	0.983
S-8	0	45	1.000
S-9	0	10	1.000

4.7.2.2 IEEE 30-bus system

The blackout rate constantly increases as k of S-k increases while k is below 8 in the IEEE 30-bus system (Table 4.7). When k is equal to or more than 8, the increase in the blackout rate is gradually saturated in the IEEE 30-bus system. k of over 8 of

Table 4.7
Dynamic simulation-based brownout and blackout cases of S-k contingency analysis using IEEE 30-bus system

S-k	Brownout (stable)	Blackout (unstable)	Blackout rate
S-1	24	4	0.143
S-2	189	87	0.315
S-3	1,164	860	0.425
S-4	5,049	5,577	0.525
S-5	15,637	26,867	0.632
S-6	35,082	99,514	0.739
S-7	57,540	288,564	0.834
S-8	69,860	665,611	0.905

S-k is not calculated because extremely heavy computation is required.

4.7.2.3 IEEE 57-bus system

The blackout rate constantly increases as k of S-k increases while k is below 5 in the IEEE 57-bus system (Table 4.8). On the other hand, the increasing speed of the blackout rate gradually declines as k of S-k increases. k of over 4 of S-k is not calculated because enormously heavy computation is required.

Table 4.8
Dynamic simulation-based brownout and blackout cases of S-k contingency analysis using IEEE 57-bus system

S-k	Brownout (stable)	Blackout (unstable)	Blackout rate
S-1	41	1	0.024
S-2	809	52	0.060
S-3	10,384	1,096	0.095
S-4	97,881	14,049	0.126

4.7.2.4 IEEE 118-bus system

The blackout rate is nearly zero when k of S-k is below 4 in the IEEE 118-bus system (Table 4.9). It is noted that the number of blackout cases is not zero when k of S-k is over 1. It can be seen that the blackout rate decreases as the grid size increases.

Table 4.9
Dynamic simulation-based brownout and blackout cases of S-k contingency analysis using IEEE 118-bus system

S-k	Brownout (stable)	Blackout (unstable)	Blackout rate
S-1	109	0	0.00000
S-2	5885	1	0.00017
S-3	209883	51	0.00024

4.7.3 Comparison of Brownout and Blackout Cases Between Power Flow Analysis and Time-domain Simulation

As shown in Fig. 4.16, the blackout and brownout combination is classified into four types (Table 4.10).

The four types shown in (Table 4.10) can be derived in the three IEEE standard systems, sorting out the results in Clauses 4.7.1 and 4.7.2. The conformity pertaining to blackout can be observed from the last two columns in Tables 4.11, 4.12, 4.13, and 4.14. The IEEE 14-bus system is the smallest grid with the smallest number

Table 4.10
Combination of blackout (critical) and brownout (non-critical) cases

Type	Power flow analysis		Dynamic simulation		Conformity
	Brownout (Convergence)	Blackout (Divergence)	Brownout	Blackout	
1	✓			✓	
2	✓		✓		✓
3		✓	✓		
4		✓		✓	✓

of substations (10 substations). On the other hand, the IEEE 118-bus system is the largest grid with the largest number of substations (109 substations). As the grid size increases, the impact of a single substation outage decreases. Therefore, the blackout rate is overall high in the IEEE 14-bus system, while the brownout rate is overall high in the IEEE 118-bus system. As shown in Table 4.14, only one blackout case for the S-2 contingency and fifty one blackout cases for the S-3 contingency.

Conformity in small grids: In the case of small grid, such as the IEEE 14-bus system, the number of Type 4 is always larger than that of Type 3. On the other hand, the number of Type 2 is mostly smaller than that of Type 1. Therefore, the blackout conformity is overall higher than the brownout conformity. The IEEE 30-bus system also exhibits the similar trend.

Conformity in large grids: In the case of large grid, such as the IEEE 57-bus system and IEEE 118-bus system, the number of Type 4 is always smaller than that

of Type 3. On the other hand, the number of Type 2 is always larger than that of Type 1. Therefore, the brownout conformity is overall higher than the blackout conformity.

In light of the above, the higher conformity is flipped between the blackout and brownout, depending on the grid size.

Table 4.11
Conformity in terms of brownout/blackout in IEEE 14-bus system

S-k	Type1	Type2	Type3	Type4	Blackout rate	
					static	dynamic
S-1	2	5	1	2	0.30	0.40
S-2	11	9	6	19	0.56	0.67
S-3	23	7	13	77	0.75	0.83
S-4	23	2	13	172	0.88	0.93
S-5	11	0	9	232	0.96	0.96
S-6	2	0	6	202	0.99	0.97
S-7	0	0	2	118	1.00	0.98
S-8	0	0	0	45	1.00	1.00
S-9	0	0	0	10	1.00	1.00

Table 4.12
Conformity in terms of brownout/blackout in IEEE 30-bus system

S-k	Type1	Type2	Type3	Type4	Blackout rate	
					static	dynamic
S-1	1	19	5	3	0.333	0.167
S-2	13	102	87	74	0.583	0.315
S-3	92	380	784	768	0.764	0.425
S-4	325	887	4,162	5,252	0.882	0.525
S-5	704	1,326	14,311	26,163	0.950	0.632
S-6	1,040	1,203	33,879	98,474	0.983	0.739
S-7	799	616	56,924	287,765	0.995	0.834
S-8	439	155	69,705	665,172	0.999	0.905

Table 4.13
Conformity in terms of brownout/blackout in IEEE 57-bus system

S-k	Type1	Type2	Type3	Type4	Blackout rate	
					static	dynamic
S-1	0	25	16	1	0.167	0.024
S-2	0	293	516	52	0.583	0.060
S-3	1	2,133	8,251	1,095	0.764	0.095
S-4	8	10,799	87,082	14,041	0.882	0.126

Table 4.14
Conformity in terms of brownout/blackout in IEEE 118-bus system

S-k	Type1	Type2	Type3	Type4	Blackout rate	
					static	dynamic
S-1	0	67	42	0	0.385	0.000
S-2	0	2,167	3,718	1	0.632	0.000
S-3	0	45,107	164,776	51	0.785	0.000

Active power output adjustability: The power flow calculation specifies a slack bus that compensates all of the deficiency of the generation and matches the generation with loads maintaining the nominal frequency. On the other hand, the time-domain simulation can consider the upper limit of the active power output of generators and represent the frequency drop. Thus, the power flow analysis can provide more optimistic results compared to the dynamic simulation. In the case of small-scale networks, a single substation outage can pose a significant active power imbalance. Therefore, this property is predominant when the grid size is small (Fig. 4.17). In other words, the power flow analysis with the superior active power-adjustability is prone to indicate optimistic results compared to the dynamic simulation in smaller grids.

It is noted that the active power output adjustability can be the same regardless of the grid size due to no upper limit of the swing generator's active power output. However, more enormous active power changes in the swing generator can also cause an overload of the transmission lines connected to the swing generator.

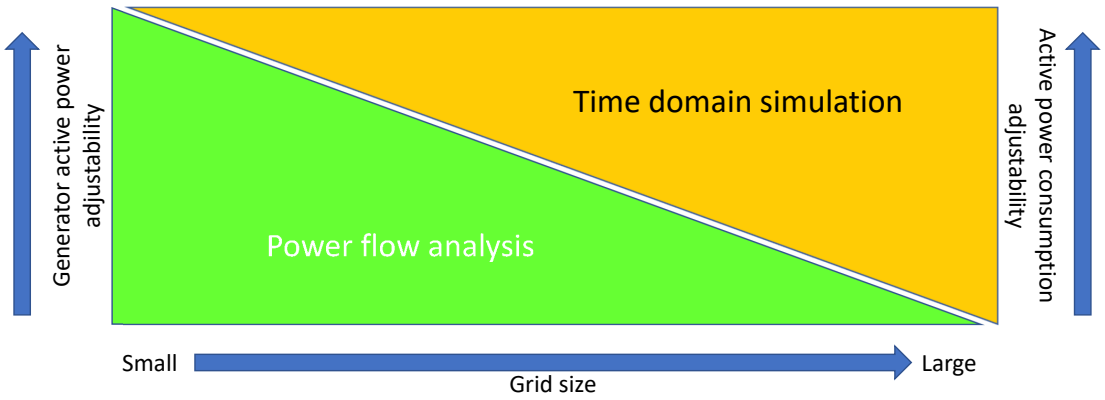


Figure 4.17: Active power output and load adjustabilities in response to grid size

Load adjustability: On the other hand, the spontaneous and forced load reduction can be precisely simulated in the time-domain simulation, while it is hard to emulate in the power flow analysis. The main point here is that active power and reactive power consumption become a function of the load bus voltage as well as frequency (see Equation 4.1), and the load bus voltage cannot be uniquely identified without an iterative approach. Because this iterative approach requires multiple power flow calculations, the power flow approach cannot generally represent the load shedding behavior. Because the load reduction can increase the possibility of containing cascaded events, the time-domain simulation can provide more optimistic results than

the power flow calculation. In large-scale networks, a single substation outage is unlikely to incur significant active power imbalance, while the grid-wide load reduction effect enhances the grid resilience in terms of frequency stability. Therefore, this property is predominant when the grid size is larger (Fig. 4.17). In other words, the time-domain simulation with the eminent load adjustability shows optimistic results compared to power flow analysis in larger networks.

Power flow calculation failure: Besides, the power flow calculation often fails when one or more bus voltage is low. Even if only one voltage cannot be converged, no power solution is obtained. There are five possible reasons (Fig. 4.18). There are many low initial voltages in the IEEE 118 bus system. Besides, there are so many synchronous condensers that provide Q power. The loss of Q support causes significant local voltage drop. Normally, power flow program cannot consider the load shedding system. Many free software cannot deal with the voltage dependent loads. Therefore, power flow analysis can show pessimistic result in the larger grid, such as the IEEE 118 bus system.

Figure 4.18: Reasons for power flow calculation failure

4.7.4 Comparison of Blackout Rate with and without Sequential S-k Contingency in IEEE 14-Bus System

The sequential coordinated attack has been a hot research topic and studied more broadly, as shown in the literature survey in Clause 1.2.4. Engineers need to differentiate between the sequential attack and the sequential event as the cascaded event.

Sequential (cyber)attack in power grids: The hacker's multiple disconnection of power equipment at a different timing, initiated by the false command injection.

Cascaded event/effect in power grids: Multiple disconnection of power equipment at a different timing, initiated by the local and system-wide protections.

The sequence of coordinated attack events is assumed to be *disconnection of one substation* (*i.e.*, single substation outage) every five seconds. The timing was carefully selected, taking into account the longest time to brownout/blackout (3 seconds) and the settling time from one operating status to another. It is emphasized that the cascaded event is always represented using the time-domain simulation unless otherwise stated about the power flow analysis.

The blackout rates with and without sequential substation attacks are the same when k of S-k is below 5 (Tab. 4.15). Once k of S-k exceeds 4, the discrepancy of the blackout rate with and without sequential substation outages gradually increases. The

Table 4.15
Dynamic simulation-based brownout and blackout cases of S-k contingency analysis with and without sequential event using IEEE 14-bus system

	W/o sequential substation outage		With sequential substation outage		Blackout rate	
	Brownout (stable)	Blackout (unstable)	Brownout (stable)	Blackout (unstable)	W/o sequential	With sequential
S-1	6	4	6	4	0.400	0.400
S-2	15	30	30	60	0.667	0.667
S-3	20	100	120	600	0.833	0.833
S-4	15	195	360	4,680	0.929	0.929
S-5	9	243	720	29,520	0.964	0.976
S-6	6	204	720	150,480	0.971	0.995
S-7	2	118	0	604,800	0.983	1.000
S-8	0	45	0	1,814,400	1.000	1.000
S-9	0	10	0	3,628,800	1.000	1.000

number of compromised high-voltage substations was seven in the Ukraine cyberattack with large blackouts in 2015. According to the grid map [153] and grid data [154] as of 2015, the number of high-voltage (equal to or over 400 kV) substations is twelve or more. Because some power stations include step-down transformers, around half of the high-voltage substations were compromised in 2015. Table 4.15 reveals that no difference of blackout rates shows if the compromised substation rate is below 50%. This means that the sequential coordinated attack does not proactively need to be considered unless extremely severe and wide substation outages are examined.

4.8 Simulation Results for R-k Contingency

Assumptions applied to this study are shown below:

- manufacturers with the cybersecurity level are the same for protection type, such as the line protection and bus protection.
- up to three protections type per substation is considered.
- priorities of the selection of the above three protection types are:

  1) Bus protection,

  2) Generator protection,

  3) Load/feeder protection.

4.8.1 Dynamic Simulation Based Blckout Rate

4.8.1.1 IEEE 14-bus system

The blackout rate slowly increases as k of R-k increases in the IEEE 14-bus system (Table 4.16). The increasing speed gradually decreases as k of R-k increases. k of over 7 of R-k is not calculated due to enormously heavy computation.

Table 4.16
Dynamic simulation-based brownout and blackout cases of R-k contingency analysis using IEEE 14-bus system

	Brownout (stable)	Blackout (unstable)	Blackout rate
R-1	23	7	0.233
R-2	258	177	0.407
R-3	1,835	2,225	0.548
R-4	9,233	18,172	0.663
R-5	35,082	107,424	0.754
R-6	104,763	489,012	0.824
R-7	249,111	1,786,689	0.878

4.8.1.2 IEEE 30-bus system

The blackout rate slowly increases as k of R-k increases in the IEEE 30-bus system (Table 4.16). Unlike the IEEE 14-bus system, the increasing speed increases as k of R-k increases. k of over 4 of R-k is not calculated due to enormously heavy computation.

Table 4.17
Dynamic simulation-based brownout and blackout cases of R-k contingency analysis using IEEE 30-bus system

	Brownout (stable)	Blackout (unstable)	Blackout rate
R-1	63	7	0.100
R-2	2,041	374	0.155
R-3	41,139	13,601	0.248
R-4	602,249	314,646	0.343

4.8.2 Comparison of Blackout Rate with and without Special Protection Scheme (SPS) in IEEE 14-Bus System

As mentioned earlier in Clause 4.1.4, the underfrequency load shedding is a representative behavior-driven SPS. Besides, loads own the load self-disconnection property. Both characteristics relates to the load adjustability that reduces the risk of blackouts along with cascaded events. As such, blackout rates of R-k contingencies are compared with and without the SPS in the IEEE 14-bus system (Table 4.18).

Table 4.18
Dynamic simulation-based brownout and blackout cases of R-k contingency analysis with and without SPS using IEEE 14-bus system

	Brownout (stable)		Blackout (unstable)		Blackout rate	
	with SPS	w/o SPS	with SPS	w/o SPS	with SPS	w/o SPS
R-1	23	22	7	8	0.233	0.267
R-2	258	241	177	194	0.407	0.446
R-3	1,835	1,732	2,225	2,328	0.548	0.573
R-4	9,233	8,830	18,172	18,575	0.663	0.678
R-5	35,082	32,579	107,424	109,927	0.754	0.771
R-6	104,763	102,414	489,012	491,361	0.824	0.828
R-7	249,111	245,830	1,786,689	1,789,970	0.878	0.879

Blackout rates with the SPS are smaller than the rates without the SPS regardless of k of R-k. However, the discrepancy of the two blackout rates is larger when k of R-k is small. This tendency is sound because the underfrequency load shedding amount has its upper limit of 25% with relative to the total load. As k of R-k increases, the active power imbalance becomes significant and it is likely to fall short of the volume of the load tripping, especially in the small grid. It can be anticipated that the SPS can be more effective for the larger grid because the required load shedding amount is highly likely to remain within the tolerance (*i.e.*, no larger than 25%).

4.9 Worst Case Scenarios and Security Protection

As shown in [17], cyberattack detection algorithms against substations have been proposed, and it is expected that the leverage of the advanced cybersecurity technologies can prevent coordinated cyberattacks against the disconnection of power equipment in substations. This technology is applied to the IED or the SCADA. As discussed earlier, the honeynet is one of the advanced and promising technologies to prevent hackers from intruding control systems or protections. On the other hand, this type of technology works after hackers successfully compromise them. Therefore, the honeynet is a cybersecurity technology for the cyber system, while the aforementioned inventing technologies are the technology for the physical system. How much these cybersecurity technologies for the physical system can reduce the blackout-scale from

a broad perspective is analyzed in this section using the IEEE 14-bus system.

4.9.1 Accounting for Deployed Security Technologies in Substations

New cybersecurity technologies in the cyber system can be deployed more widely, while such technologies in the physical system cannot be developed at one time due to the higher hardware dependency. Such a new cybersecurity technologies for physical systems (hereafter, new security technologies for physical systems) need to be applied from one substation to another. In the case study, one substation is assumed to employ the new security technologies for physical systems. If this technology can be considered to prevent hackers from switching actions in the specific substation, that substation is out of the list of the contingency analysis. Thus, the loss of electricity (LOE) is likely to decrease when one substation is removed from the contingency list. For example, if the advanced technology is only available for substation 3, a S-k contingency that contains substation 3 in the combination changes to a S-k-1 contingency that excludes substation 3 in the combination. The example change is shown below:

Example of S-2: From "SS03-SS10" to "SS10"

Example of S-3: From "SS03-SS04-SS05" to "SS04-SS05"

Example of S-5: From "SS02-SS03-SS12-SS13-SS14" to "SS02-SS12-SS13-SS14"

4.9.2 Case Study in IEEE 14-Bus System

The loss of electricity in the IEEE 14-bus system discussed in this case study is calculated as the mean value of the LOE for 1022 cases (*i.e.*, S-1, S-2, ... S-9 contingencies), 94.4%. In the case of employing the new security technologies for physical systems at one substation, the LOE decreases by 0.1-21%, depending on the substation (Fig. 4.19). Fig. 4.19 reveals that substation 4 is the most effective substation to introduce new security technologies for physical systems. The three substations that can obtain a higher effect of introducing the technology have a synchronous condenser. On the other hand, substations that can create less effect of introducing the technology have loads only. Because only substations 1 and 2 have a synchronous generator, it is observed that the IEEE 14-bus system is more vulnerable to the loss of synchronous condensers compared to the loss of synchronous generators.

Although all contingencies should be considered to estimate the averaged LOE, k f S-k can be capped at a value that is less than ten. In this case, the LOE per se can change depending on the cap of k. Therefore, the reduction rate with relative to the LOE that corresponds the cap of k is more comprehensive indicator. When the cap of k decreases from nine to two, the reduction rate mentioned above increases (Table 4.20).

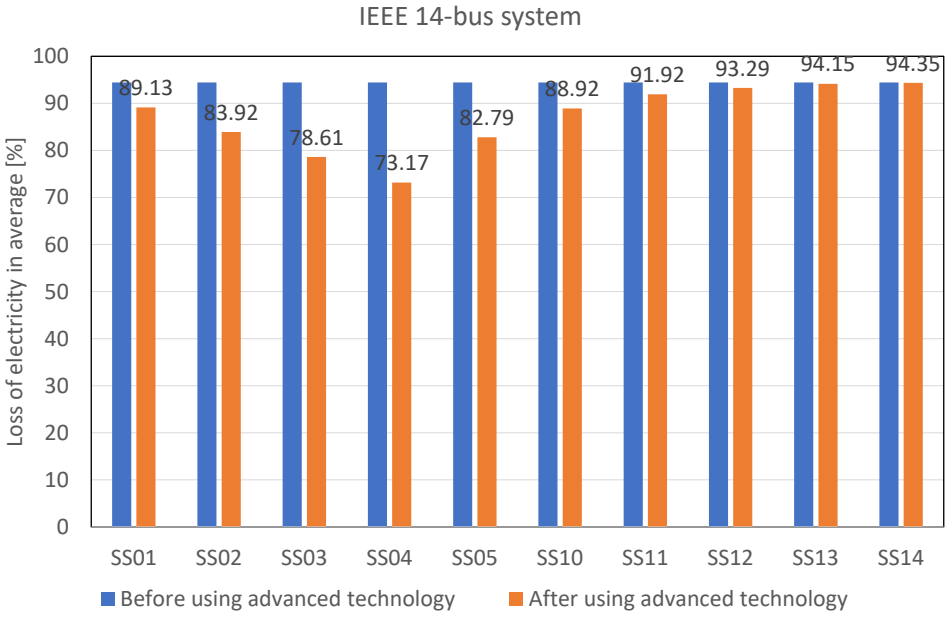


Figure 4.19: Loss of electricity with and without new cybersecurity technology for physical systems in a single substation

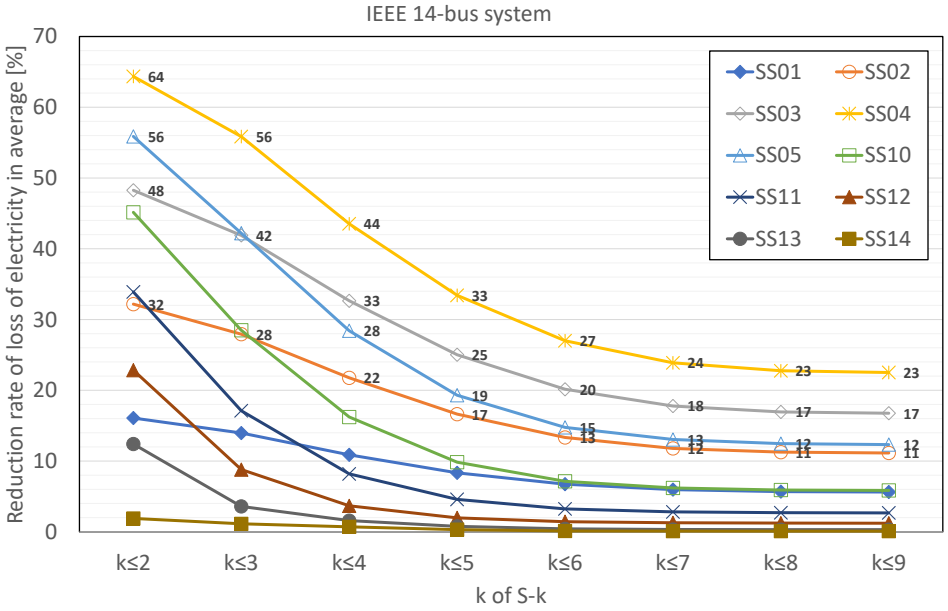


Figure 4.20: Loss of electricity reduction rate with new cybersecurity technology for physical systems

Compared to the honeynet's improvement in cybersecurity in Fig. 3.2, the improvement in cybersecurity using the new cybersecurity technology for physical systems looks overall smaller. It is noted that the honeynet is assumed to employ the prevention function, and the improvement property of honeynet with the prevention function largely depends on the used parameters in the cyber-net model. Because some substations exponentially increase the LOE reduction rate for the cap of k, rigorous cost-effective analysis is also required when selecting the new cybersecurity technology.

4.10 Summing Up for the Systemic Risks

4.10.1 IEEE 14-bus system

Once the steady-state probability of cyberattacks against a designated substation and the loss of electricity for the same substation outage, the economical impact in the steady-state probability manner may be derived multiplying both values Table 4.19). Although the absolute value does not have a specific meaning, the critical level of substations from insurance perspectives may be ranked using those values. The result shows that substations 3 and 5 are the critical substations (Fig. 4.21).

It can be realized that substations 10, 11, 12 and 14 are easy to be compromised

Table 4.19
Steady-state probability of loss of electricity for single substation attack in IEEE 14-bus system

Substation name	Steady-state probability of cyberattack	Loss of electricity	Steady-state probability of loss of electricity
SS01	1.59E-07	100	1.59E-05
SS02	1.20E-07	100	1.20E-05
SS03	1.90E-07	100	1.90E-05
SS04	1.75E-07	100	1.75E-05
SS05	1.97E-07	9.68	1.91E-06
SS10	2.35E-07	3.01	7.07E-07
SS11	2.35E-07	1.29	3.03E-07
SS12	2.35E-07	2.15	5.05E-07
SS13	1.90E-07	4.88	9.27E-07
SS14	2.35E-07	5.09	1.20E-06

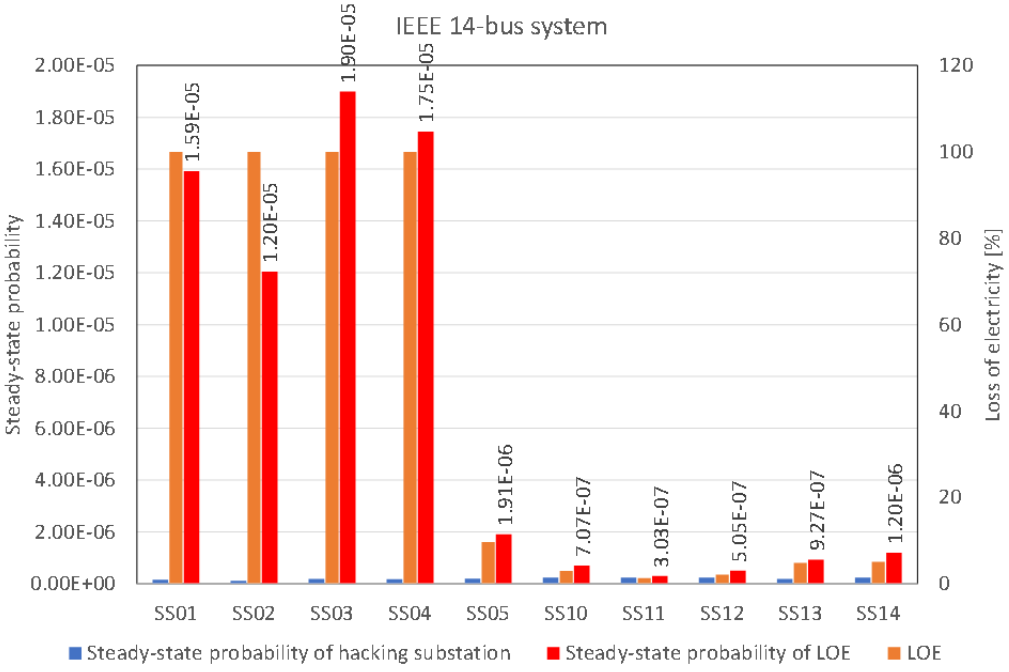


Figure 4.21: Steady-state probability of loss of electricity for single substation attack in IEEE 14-bus system

compared to the rest substations. However, the impact of those substation attacks is much smaller than that of substations 1, 2, 3, and 4. Therefore, the final economical loss needs to be derived from the cyber risk probability and the impact of the cyberattack in a holistic manner.

4.10.2 IEEE 30-bus system

In the same manner, the steady-state probability manner may be derived (Table 4.20). The result shows that substations 4 and 1 are critical (Fig. 4.22).

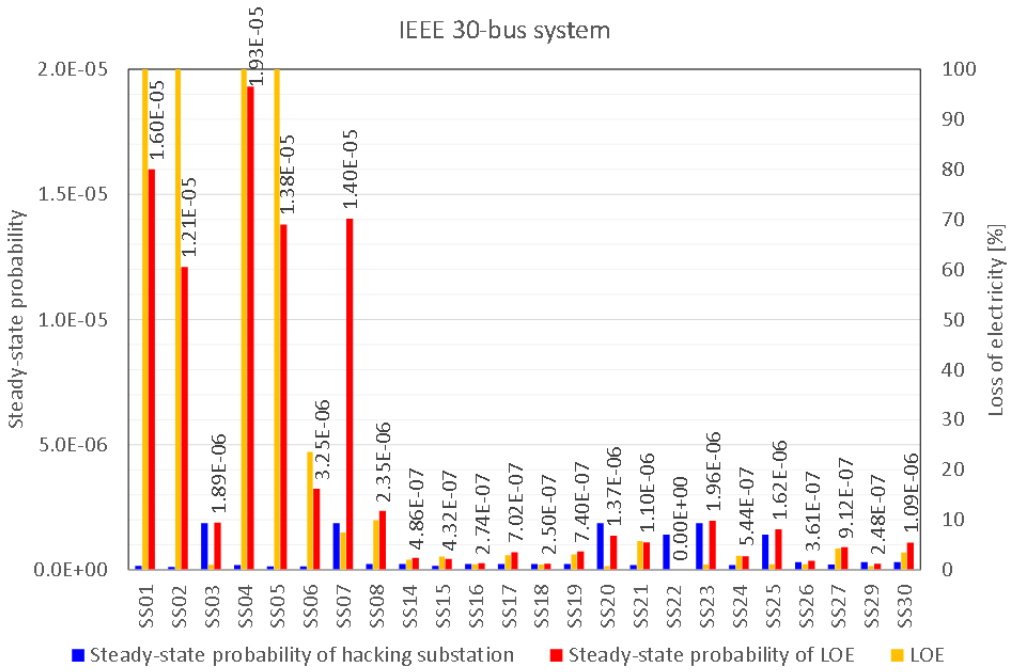


Figure 4.22: Steady-state probability of loss of electricity for single substation attack in IEEE 30-bus system

It can be realized that substations 3, 7, 20, and 23 are easy to compromise than the rest substations. However, those substation attacks' impact is much smaller than that of substations 1, 2, 4, and 5. After the final economic loss is derived from the cyber risk probability and the impact of the cyberattack in a holistic manner, it may be concluded that substations 4 is the most critical substation.

Table 4.20
Steady-state probability of loss of electricity for single substation attack in IEEE 30-bus system

Substation name	Steady-state probability of cyberattack	Loss of electricity	Steady-state probability of loss of electricity
SS01	1.60E-07	100.	1.60E-05
SS02	1.21E-07	100.	1.21E-05
SS03	1.87E-06	1.01	1.89E-06
SS04	1.93E-07	100.	1.93E-05
SS05	1.38E-07	100.	1.38E-05
SS06	1.38E-07	23.54	3.25E-06
SS07	1.87E-06	7.50	1.40E-05
SS08	2.38E-07	9.89	2.35E-06
SS14	2.38E-07	2.04	4.86E-07
SS15	1.60E-07	2.70	4.32E-07
SS16	2.38E-07	1.15	2.74E-07
SS17	2.38E-07	2.95	7.02E-07
SS18	2.38E-07	1.05	2.50E-07
SS19	2.38E-07	3.11	7.40E-07
SS20	1.87E-06	0.73	1.37E-06
SS21	1.91E-07	5.75	1.10E-06
SS22	1.41E-06	0.00	0.00E+00
SS23	1.87E-06	1.05	1.96E-06
SS24	1.91E-07	2.85	5.44E-07
SS25	1.41E-06	1.15	1.62E-06
SS26	3.14E-07	1.15	3.61E-07
SS27	2.14E-07	4.26	9.12E-07
SS29	3.14E-07	0.79	2.48E-07
SS30	3.14E-07	3.47	1.09E-06

Chapter 5

Conclusion and Future Work

The compilation and analysis of anomaly data statistics extracted from the cyber system in IP-based substations are critical to the understanding of security health within the private network. Establishing steady-state probabilities based on the network architecture, security technologies, as well as characterizing intrusion behaviors, are the essential subjects to estimate security risks. This dissertation advances the procedure to reflect on the steady-state probabilities of switching substation attacks within the existing implementation of security protection, using Petri net models. This also provides a guideline on the estimation of model parameters in the specific substation topology and protective IEDs.

5.1 Contribution of Cyber-Net Model

The first work enables us to clarify the probability of cyberattacks against SCADA systems and IEDs from steady-state probability perspectives. The major contributions of the Petri net model are:

- The proposed Petri net model can contrast the switching attack probabilities with and without advanced cybersecurity technologies such as the honeynet.
- The created Petri net model is further expanded to derive the probability of IED attacks.
- The developed Petri net model can derive the different probability of substation attacks depending on protection type, relay type, and number of relay settings.

Specifically, the Petri net model can specify the substation that power engineers should pay attention from cybersecurity point of view.

However, the developed model has a limitation. It is noted that the proposed Petri net model is based on the Markov property for state transitions. The GSPN is applicable only when the holding time, such as the sojourn time, in each state, is assumed to be either zero or exponentially distributed. Future research includes establishing other statistical distributions. In addition, enhancing the modeling complexity in terms of

the size of the specific modeling can increase computational time.

5.2 Contribution of Dynamic Simulation Model

The dynamic behavior caused by the switching cyberattack against substations is different from the behavior caused by the general system fault (short circuit fault). As the time-domain simulation is more time-consuming than the power flow analysis, minimizing the leveraged control models and protection models that can adequately represent the cascaded behavior in the grid is vital to ensure the balance between the accuracy and the efficiency of this work.

The control and protection models that play an essential role in representing cascaded events are carefully distilled (Tabs. 5.1 and 5.2). Not only the local protections but also wide-area protections, *i.e.*, the SPS is verified. The substation attack does not accompany system faults. Therefore, the necessary control and protection models have not yet been studied and clarified exhaustively. Representative stability, such as transient stability, voltage stability, and frequency stability, are reviewed.

The various sensitivity studies for S-k and R-k contingency analyses using the properly selected models shown in Tabs. 5.1 and 5.2 generate the following beneficial findings:

Table 5.1
Necessary protective relay for substation attack study

Component to be protected	Protective relay type
Synchronous generator	Underfrequency relay Overfrequency relay Out-of-step relay
Synchronous condenser	Underfrequency relay Overfrequency relay Overvoltage relay
Transformer	Overvoltage relay
Load	Underfrequency relay Undervoltage relay*
Network (Line)	Out-of-step relay

*: Self-disconnection characteristics may be applied instead of undervoltage relay.

Table 5.2
Necessary controller for substation attack study

Component	Controller
Synchronous generator	AVR(+PSS) Over excitation limiter (OEL) Primary Frequency Controller
Synchronous condenser	AVR
Transformer	Shunt reactor/capacitor
Load	N/A
Network (Line)	FACTS (if any)

- Power flow analysis tends to bring pessimistic results (*i.e.*, more unstable), especially when the number of substation/relay outage is small.

- Simultaneous substation/relay outage is prone to present optimistic results (*i.e.*, more stable), only when the number of substation/relay outage becomes large.

- SPS (underfrequency relay) plays the important role to prevent grid stability from deteriorating, especially when the number of substation/relay outage is small.

Although there are available sources to obtain the IEEE standard models' input data, simulation data were set at different platforms/tools, and the derived power flow solution (especially voltage angles) is not always the same. Besides, quite limited data are provided for the dynamic simulation. If at all, no rationale of the provided parameters is clarified. This dissertation uses a commercially available, proven time-domain simulation tool that has been used by commercial power companies in Japan. Then, the exact condition and parameters are rigorously illustrated in Appendix B.

5.3 Combinatorial Efficiency

Although this dissertation provides the imperative control and protection models that are culled from the available numerical models, further efforts to lessen the computation burden are required, especially for larger power grids. There are some approaches to cope with this technical challenge.

- Reduce the number of contingency cases,
- Predict the loss of electricity for the larger k of S - k based on the loss of electricity for the smaller k of S - k.

The effective leverage of the power flow analysis results can be a promising candidate

to resolve the first problem. On the other hand, the use of the state-of-the-art techniques, such as the machine-learning algorithm can be a promising candidate to tackle the second problem. Establishing a reliable approach to skip non-critical substation is also one of the crucial steps to decrease the calculation cost. To achieve this, the following research studies on identifying critical substations with their ranking must become pivotal.

5.4 Actuarial Framework Implementation

Capturing the risks of switching attack can be further extended for estimating cyber insurance premiums because such a risk is generally derived from the steady-state probability of anomalies and the impact of the switching attack. Other combinations, such as one or more outages of interconnected substations due to false data injection attacks, should be considered in the proposed risk-based framework. Asset owners can also consider implementing their in-house cyber analytics to understand and implement security policies more effectively.

References

[1] North American Reliability Corporation, "CIP standards." [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[2] Federal Departments and Agencies, "Draft national infrastructure protection plan," Nov. 2005. [Online]. Available: https://fas.org/irp/agency/dhs/nipp110205.pdf.

[3] R. Heidorn Jr., "NERC seeks $10M fine for duke energy security lapses," Feb. 2019. [Online]. Available: https://www.rtoinsider.com/nerc-fine-duke-energy-cip-110308/.

[4] Center for Strategic and International Studies (CSIS), "Significant cyber incidents since 2006," Feb. 2019. [Online]. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf.

[5] R. Bulbul, P. Sapkota, C.-W. Ten, L. Wang, and A. Ginter, "Intrusion evaluation of communication network architectures for power substations,"

IEEE Trans. Power Del., vol. 30, no. 3, pp. 1372–1382, June 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7054545

[6] T. H. Morris, A. K. Srivastava, B. Reaves, K. Pavurapu, S. Abdelwahed, R. Vaughn, W. McGrew, and Y. Dandass, "Engineering future cyber-physical energy systems: Challenges, research needs, and roadmap," in *41st North American Power Symposium*, Starkville, MS, USA, Oct. 2009. [Online]. Available: https://ieeexplore.ieee.org/document/5484019.

[7] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber security of water scada systems—part I: Analysis and experimentation of stealthy deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1963–1970, Sep. 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6303885.

[8] S. Amin and X. Litrico and S. S. Sastry and A. M. Bayen, "Cyber security of water scada systems—part II: Attack detection using enhanced hydrodynamic models," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, p. 1679–1693, Sep. 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6307833.

[9] The Department of Homeland Security, "Critical infrastructure protection DHS has made progress in enhancing critical infrastructure assessments, but additional improvements are needed," July 2016. [Online]. Available: https://www.gao.gov/assets/680/678344.pdf.

[10] NERC Board of Trustees, "Reliability standards for the bulk electric systems of north america," May 2017. [Online]. Available: http://www.nerc.com/pa/Stand/ReliabilityStandardsCompleteSet/RSCompleteSet.pdf.

[11] Critical Infrastructure Protection Committee (CIPC), "Cybersecurity – BES cyber system categorization," Oct. 26 2012. [Online]. Available: http://www.netsectech.com/wp-content/uploads/2013/05/Version-5-of-the-NERC-CIP-Cyber-Security-Standards.pdf.

[12] K.-P. Brand, V. Lohmann, and W. Wimmer, *Substation Automation Handbook*. Utility Automation Consulting Lohmann, 2003.

[13] IEC, "Communication networks and systems for power utility automation -part 90-4: Network engineering guidelines," International Electrotechnical Commission, Tech. Report TR 61850-90-4:2013, Aug. 2013.

[14] *C37.240-2014 - IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems*, IEEE, 2014. [Online]. Available: https://ieeexplore.ieee.org/document/7024885.

[15] H. Wardak, S. Zhioua, and A. Almulhem, "PLC access control: a security analysis," in *Proc. 2016 World Congress on Industrial Control Systems Security (WCICSS)*, London, UK, Dec. 2016, pp. 1–6.

[16] S. Bricker, T. Gonen, and L. Rubin, "Substation automation technologies and

advantages," *IEEE Comput. Appl. Power*, vol. 14, no. 3, pp. 31–37, Jul. 2001. [Online]. Available: https://ieeexplore.ieee.org/document/952934

[17] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *Innovative Smart Grid Technologies (ISGT), 2014 IEEE PES*, Feb. 2014, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/6816375

[18] L. Spitzner, "The honeynet project: Trapping the hackers," *IEEE Security Privacy*, vol. 1, no. 2, pp. 15–23, Mar. 2003. [Online]. Available: http://dx.doi.org/10.1109/MSECP.2003.1193207.

[19] L. R. Even. (July. 2000) Honeypot systems explained. [Online]. Available: https://www.sans.org/security-resources/idfaq/honeypot3.php.

[20] M. Nawrocki, M. Wahlisch, T. C. Schmidty, C. Keilz, and J. Schonfelder. (Aug. 2016) A survey on honeypot software and data analysis. Cornell University. [Online]. Available: https://arxiv.org/pdf/1608.06249.

[21] K. Yamashita, C.-W. Ten, Y. Rho, L. Wang, W. Wei, and A. F. Ginter, "Measuring systemic risk of switching attacks based on cybersecurity technologies in substations," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4206–4219, Nov. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9078877.

[22] T. Murata, "Petri nets: Properties, analysis and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989. [Online]. Available: https://ieeexplore.ieee.org/document/24143

[23] F. Bause and P. S. Kritzinger, *Stochastic Petri Nets*, 2nd ed. Vieweg+Teubner Verlag, 2002.

[24] C. A. Petri, "Kommunikation mit automaten," in *Ph.D. Dissertation*, vol. 3, Bonn:Institut für Instrumentelle Mathematik, Jun. 1962.

[25] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA system," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008. [Online]. Available: https://ieeexplore.ieee.org/document/4652578.

[26] M. A. Berger, *An Introduction to Probability and Stochastic Processes*, 1st ed. Springer, New York, NY, 1993.

[27] C.-S. Cho, W.-H. Chung, and S.-Y. Kuo, "Cyber-physical security and dependability analysis of digital control systems in nuclear power plants," *IEEE Trans. Syst., Man, Cybern.*, vol. 46, no. 3, pp. 356–369, 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7192645

[28] R. Zeng, Y. Jiang, C. Lin, and X. Shen, "Dependability analysis of control center networks in smart grid using stochastic Petri nets," *IEEE Trans.*

Parallel Distrib. Syst., vol. 23, no. 9, pp. 1721–1730, 2012. [Online]. Available: https://ieeexplore.ieee.org/document/6152095

[29] R. Mitchell and I.-R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Trans. Rel.*, vol. 62, no. 1, pp. 199–210, March 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6423246

[30] D. Verneza, D. Buchsb, and G. Pierrehumberta, "Perspectives in the use of coloured petri nets for risk analysis and accident modelling," *Safety Science*, vol. 41, no. 5, pp. 445–463, June 2003.

[31] V. Sharma, G. Choudhary, Y. Ko, and I. You, "Behavior and vulnerability assessment of drones-enabled industrial internet of things (IIoT)," *IEEE Access*, vol. 6, pp. 43 368–43 383, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8411430

[32] London Economics International LLC, "Estimating the value of lost load," Jun. 17, 2013. [Online]. Available: http://www.ercot.com/content/gridinfo/resource/2015/mktanalysis/ERCOT_ValueofLostLoad_LiteratureReviewandMacroeconomic.pdf.

[33] European Network and Information Security Agency, "Incentives and barriers of the cyber insurance market in europe," Jun. 28 2012. [Online]. Available: http://www.biztositasiszemle.hu/files/201207/cyber_insurance_market.pdf.

[34] J. F. Anderson and R. L. Brown. (2005) Risk and insurance. Education And Examination Committee of the Society Actuaries. [Online]. Available: https://www.soa.org/files/pdf/P-21-05.pdf.

[35] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6695779

[36] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A smart grid vulnerability analysis framework for coordinated variable structure switching attacks," in *Proc. 2012 IEEE Power and Energy Society General Meeting*, San Diego, CA, USA, July 2012. [Online]. Available: https://ieeexplore.ieee.org/document/6344617

[37] A. Farraj, E. Hammad, A. A. Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1846–1855, July 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7127052

[38] S. Z. Yong, M. Zhu, and E. Frazzoli, "Resilient state estimation against switching attacks on stochastic cyber-physical systems," in *2015 IEEE 54th Annual Conference on Decision and Control (CDC)*, Dec. 2015, pp. 5162–5169. [Online]. Available: https://ieeexplore.ieee.org/document/7403027

[39] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 56–168, Aug. 2017.

[40] A. Huseinovic, S. Mrdovic, K. Bicakci, and S. Uludag, "A survey of denial-of-service attacks and solutions in the smart grid," *IEEE Access*, vol. 8, pp. 177 447–177 470, Sep. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9205862.

[41] Z. Yang, C.-W. Ten, and A. Ginter, "Extended enumeration of hypothesized substations outages incorporating overload implication," *IEEE Trans. on Smart Grid*, vol. 9, no. 6, pp. 6929–6938, Nov. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/7983394

[42] C.-W. Ten, A. Ginter, and R. Bulbul, "Cyber-based contingency analysis," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3040–3050, Jul. 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7284712

[43] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, April 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8090056.

[44] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 156–168, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0378779617301700.

[45] J. F. Bard, *Practical Bilevel Optimization -Algorithms and Applications*, 1st ed. USA.: Springer, 1998.

[46] R. D. Christie, "Power systems test case archive," Aug. 1999. [Online]. Available: http://labs.ece.uw.edu/pstca/pf14/pg_tca14bus.htm.

[47] Z. Liu and L. Wang, "Defense strategy against load redistribution attacks on power systems considering insider threats," *IEEE Trans. on Smart Grid*, Sep. 2020, early access. [Online]. Available: https://ieeexplore.ieee.org/document/9195020.

[48] C. Chen, M. Cui, X. Wang, K. Zhang, and S. Yin, "An investigation of coordinated attack on load frequency control," *IEEE Access*, vol. 6, pp. 30 414–30 423, June 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8374820.

[49] J. Fu, L. Wang, B. Hu, K. Xie, H. Chao, and P. Zhou, "A sequential coordinated attack model for cyber-physical system considering cascading failure and load redistribution," in *2018 2nd IEEE conference on Energy*

Internet and Energy System Integration, Beijing, China, Dec. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8582135.

[50] I. Dobson, B. Carreras, V. Lynch, and D. Newman, "An initial model fo complex dynamics in electric power system blackouts," in *the 34th Annual Hawaii International Conference on System Sciences*, Hawai, USA., Jan. 2001. [Online]. Available: https://ieeexplore.ieee.org/document/926274.

[51] T. Athay, R. Podmore, and S. Virmani, "A practical method for the direct analysis of transient stability," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-98, no. 2, pp. 573–584, March 1979. [Online]. Available: https://ieeexplore.ieee.org/document/4113518.

[52] A. Pai, *Energy Function Analysis for Power System Stability*. Springer, 1989.

[53] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 17, pp. 4332–4341, July 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8556464.

[54] Y. M. Khaw, A. A. Jahromi, M. F. M. Arani, D. Kundur, S. Sanner, and M. Kassouf, "Preventing false tripping cyberattacks against distance relays: A deep learning approach," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*,

Beijing, China, Oct. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8909810.

[55] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning (Adaptive Computation and Machine Learning series)*. The MIT Press, 2016.

[56] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward threat of implementation attacks on substation security: Case study on fault detection and isolation," *IEEE Trans. on Industrial Informatics*, vol. 14, no. 6, pp. 2442–2451, June 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8097030.

[57] S. Paul, Z. Ni, and F. Ding, "An analysis of post attack impacts and effects of learning parameters on vulnerability assessment of power grid," in *Smart Grid Technologies Conference (ISGT) 2020 IEEE Power & Energy Society Innovative*, Washington DC, USA., 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9087639.

[58] S. Weerasinghe, T. Alpcan, S. M. Erfani, C. Leckie, P. Pourbeik, and J. Riddle, *Deep Learning Based Game-Theoretical Approach to Evade Jamming Attacks*. Cham, Switzerland: Springer, 2018.

[59] Z. Zhang, S. Huang, F. Liu, and S. Mei, "Pattern analysis of topological attacks in cyber-physical power systems considering cascading outages,"

IEEE Access, vol. 8, pp. 134 257–134 267, July 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9131768.

[60] L. Wang, Z. Qu, Y. Li, K. Hu, J. Sun, K. Xue, and M. Cui, "Method for extracting patterns of coordinated network attacks on electric power cps based on temporal–topological correlation," *IEEE Access*, vol. 8, pp. 57 260–57 272, March 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9042337.

[61] J. D. Young and E. S. Jr, "Introduction to temporal bayesian networks," in *The Seventh Midwest AI and Cognitive Science Conference*, April 1996. [Online]. Available: https://www.researchgate.net/profile/Eugene_Santos2/publication/267965687_Introduction_to_Temporal_Bayesian_Networks_y/links/54b9212e0cf28faced626fb0/Introduction-to-Temporal-Bayesian-Networks-y.pdf.

[62] C. C. Sun, J. Hong, and C. C. Liu, "A coordinated cyber attack detection system (ccads) for multiple substations," in *Power System Computation Conference (PSCC)*, June 2016, pp. 114–129. [Online]. Available: https://ieeexplore.ieee.org/document/7540902.

[63] Z. Liu and L. Wang, "Leveraging network topology optimization to strengthen power grid resilience against cyber-physical attacks," *IEEE*

Trans. on Smart Grid, Oct. 2020, early access. [Online]. Available: https://ieeexplore.ieee.org/document/9210594.

[64] M. Heidarifar and H. Ghasemi, "A network topology optimization model based on substation and node-breaker modeling," *IEEE Trans. on Power Syst.*, vol. 31, no. 1, pp. 247–255, Jan. 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7038226.

[65] R. D. Christie, "Power systems test case archive," Aug. 1999. [Online]. Available: http://labs.ece.uw.edu/pstca/pf57/pg_tca57bus.htm.

[66] ——, "Power systems test case archive," Aug. 1999. [Online]. Available: http://labs.ece.uw.edu/pstca/pf118/pg_tca118bus.htm.

[67] M. Touhiduzzaman, A. Hahn, and A. K. Srivastava, "A diversity-based substation cyber defense strategy utilizing coloring games," *IEEE Trans. on Smart Grid*, vol. 10, no. 5, pp. 5405–5415, Sep. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8538008.

[68] M. Zhang, L. Wang, S. Jajodia, A. Singhal, and M. Albanese, "Network diversity: A security metric for evaluating the resilience of networks against zero-day attacks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, p. 1071–1086, May 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7378495.

[69] P. N. Panagopoulou and P. G. Spirakis, "A game theoretic approach for efficient graph coloring," in *Algorithms and Computation*, S.-H. Hong, H. Nagamochi, and T. Fukunaga, Eds. Berlin, Heidelberg: Springer, 2008. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-92182-0_19.

[70] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. on Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7185427.

[71] P. Xua and L. Wang, "An exact algorithm for the bilevel mixed integer linear programming problem under three simplifying assumptions," *Computers & Operations Research*, vol. 41, pp. 309–318, Jan. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0305054813001950.

[72] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense for detecting coordinated cyber-physical attacks in power grids," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*, Beijing, China, Oct. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8909767.

[73] Z. Liu, W. Wei, L. Wang, C.-W. Ten, and Y. Rho, "An actuarial framework for power system reliability considering cybersecurity threats,"

IEEE Trans. on Power Syst., Aug. 2020, early access. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9174921.

[74] Z. Yang, M. Campbell, C.-W. Ten, Y. Rho, L. Wang, and W. Wei, "Premium calculation for insurance business based on cyber risks in ip-based power substations," *IEEE Access*, vol. 8, pp. 78 890–78 900, April 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9069962.

[75] R. Kaas, M. Goovaerts, J. Dhaene, and M. Denuit, *Modern Actuarial Risk Theory*. Berlin, Heidelberg: Springer, 2008.

[76] P. Lau, W. Wei, L. Wang, Z. Liu, and C.-W. Ten, "Concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks," *IEEE Trans. on Smart Grid*, vol. 11, no. 5, pp. 4403–4414, Sep. 2020, early access. [Online]. Available: https://ieeexplore.ieee.org/document/9087864.

[77] D. Kar, T. H. Nguyen, F. Fang, M. Brown, A. Sinha, M. Tambe, and A. X. Jiang, *Trends and Applications in Stackelberg Security Games*, 1st ed. Cham, Switzerland: Springer, 2017.

[78] J. Janssen, *Semi-Markov Models -Theory and Applications*, 1st ed. USA.: Springer, 1986.

[79] H. Yang, J. Qiu, K. Meng, J.-H. Zhao, Z.-Y. Dong, and M. Lai, "Insurance strategy for mitigating power system operational risk introduced by wind

power forecasting uncertainty," *Renewable Energy*, vol. 89, pp. 606–615, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0960148115305176.

[80] M. Ni, M. Li, J. Li, Y. Wu, and Q. Wang, "Concept and research framework for coordinated situation awareness and active defense of cyber-physical power systems against cyber-attacks," *Journal of Modern Power Systems and Clean Energy*, June 2020, early access. [Online]. Available: https://ieeexplore.ieee.org/document/9127768.

[81] B. Chen, K. L. Butler-Purry, S. Nuthalapati, and D. Kundur, "Network delay caused by cyber attacks on svc and its impact on transient stability of smart grids," in *Proc. 2014 IEEE Power and Energy Society General Meeting*, National Harbor, MD, USA, July 2014. [Online]. Available: https://ieeexplore.ieee.org/document/6938963.

[82] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber attacks on transient stability of smart grids with voltage support devices," in *Proc. 2013 IEEE Power and Energy Society General Meeting*, Vancouver, BC, Canada, July 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6672740.

[83] B. Chen, K. L. Butler-Purry, and D. Kundur, "Impact analysis of transient stability due to cyber attack on facts devices," in *Proc. North Amer.*

Power Symp. (NAPS), Manhattan, KS, USA, Sep. 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6666849.

[84] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, March 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8248780.

[85] V. Terzija, G. Valverde, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, "Wide-area monitoring, protection, and control of future electric power networks," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80–93, Jan. 2011. [Online]. Available: https://ieeexplore.ieee.org/document/5549870.

[86] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, P. B. B. Pranggono, and H. Wang, "Intrusion detection system for network security in synchrophasor systems," in *IET International Conference on Information and Communications Technologies (IETICT 2013)*, Beijing, China, April 2013, pp. 246–252. [Online]. Available: https://ieeexplore.ieee.org/document/6617502.

[87] Y. Li, P. Zhang, and L. Ma, "Denial of service attack and defense method on load frequency control system," *Journal of the Franklin Institute*, vol. 356, no. 15, pp. 8625–8645, Oct. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0016003219306106.

[88] J. Wei and D. Kundur, "A flocking-based model for dos-resilient communication routing in smart grid," in *2012 IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, USA, Dec. 2012, pp. 3519–3524. [Online]. Available: https://ieeexplore.ieee.org/document/6503660.

[89] K. Demir and N. Suri, "Towards DDoS attack resilient wide area monitoring systems," in *ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and Security*, New York, USA, Aug. 2017. [Online]. Available: https://dl.acm.org/doi/10.1145/3098954.3103164.

[90] M. R. Mengis and A. Tajer, "Data injection attacks on electricity markets by limited adversaries: Worst-case robustness," *IEEE Trans. on Smart Grid*, vol. 9, no. 6, pp. 5710–5720, Nov. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/7903742.

[91] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact dynamic game strategy for jamming attack in electricity market," *IEEE Trans. on Smart Grid*, vol. 6, no. 5, pp. 2273–2282, Sep. 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7050307.

[92] Z. Alavikia, N. Mozayani, J. Shahbazi, and F. Alavikia, "Utilizing an agent based negotiation mechanism to defend against jamming attack in smart grid power market," in *Proc. 2018 9th International Symposium on*

Telecommunications (IST), Tehran, Iran, Dec. 2018, pp. 45–52. [Online]. Available: https://ieeexplore.ieee.org/document/8660977.

[93] M. Attia, S. M. Senouci, H. Sedjelmaci, E.-H. Aglzim, and D. Chrenko, "An efficient intrusion detection system against cyber-physical attacks in the smart grid," *Computers Electrical Engineering*, vol. 68, pp. 499–512, May 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790617332068.

[94] M. McKeay and A. Fakhreddine, "State of the internet - security web attack," Akamai, Tech. Rep., 2018. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf.

[95] S. Goel and Y. Hong, "Security challenges in smart grid implementation," in *Smart Grid Security*, S. Goel, Y. Hong, V. Papakonstantinou, and D. Kloza, Eds. Verlag, London: Springer UK, 2015, pp. 1–39. [Online]. Available: https://www.springer.com/gp/book/9781447166627.

[96] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, USA, Oct. 2010, pp. 350–355. [Online]. Available: https://ieeexplore.ieee.org/document/5622068.

[97] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cardenas, and J. G. Jetcheva, "Ami threats, intrusion detection requirements and deployment recommendations," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, Tainan, Taiwan, Nov. 2012, p. 395–400. [Online]. Available: https://ieeexplore.ieee.org/document/6486016.

[98] D. Jin, Y. Zheng, H. Zhu, D. M. Nicol, and L. Winterrowd, "Virtual time integration of emulation and parallel simulation," in *2012 ACM/IEEE/SCS 26th Workshop on Principles of Advanced and Distributed Simulation*, Zhangjiajie, China, July 2012, pp. 201–210. [Online]. Available: https://ieeexplore.ieee.org/document/6305913.

[99] S. Rana, H. Zhu, C. W. Lee, D. M. Nicol, and I. Shin, "The not-so-smart grid: Preliminary work on identifying vulnerabilities in ansi c12.22," in *2012 IEEE Globecom Workshops*, Anaheim, CA, USA, Dec. 2012, pp. 1514–1519. [Online]. Available: https://ieeexplore.ieee.org/document/6477810.

[100] W. G. Temple, B. Chen, and N. O. Tippenhauer, "Delay makes a difference: Smart grid resilience under remote meter disconnect attack," in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Vancouver, BC, Canada, Oct. 2013, pp. 462–467. [Online]. Available: https://ieeexplore.ieee.org/document/6688001.

[101] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *Journal of Network and Computer Applications*, vol. 59, pp. 325–332, May 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804515000880.

[102] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Sep. 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7857804.

[103] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. on Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6400273.

[104] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing gps receiver clock offset of phasor measurement units," *IEEE Trans. on Power Systems*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6451170.

[105] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against gps spoofing attacks on pmus in smart grids," *IEEE Trans. on Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov. 2015. [Online]. Available: https://ieeexplore.ieee.org/document/6887343.

[106] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for ptp delay attack in an iec 61850 substation," *IEEE Trans. on Smart Grid*, vol. 9, no. 5, pp. 3954–3965, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/7797198.

[107] M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "Vulnerability of synchrophasor-based wampac applications' to time synchronization spoofing," *IEEE Trans. on Smart Grid*, vol. 9, no. 5, pp. 4601–4612, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/7845713.

[108] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1952–1973, Feb. 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7397831.

[109] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "Gps spoofing attack characterization and detection in smart grids," in *2016 IEEE Conference on Communications and Network Security (CNS)*, Philadelphia, PA, USA, Oct. 2016, p. 391–395. [Online]. Available: https://ieeexplore.ieee.org/document/7860525.

[110] S. B. Andrade, J.-Y. L. Boudec, E. Shereen, G. Dan, M. Pignati, and M. Paolone, "A continuum of undetectable timing-attacks on pmu-based linear state-estimation," in *2017 IEEE International Conference on Smart*

Grid Communications (SmartGridComm), Dresden, Germany, Oct. 2017, pp. 476–479. [Online]. Available: https://ieeexplore.ieee.org/document/8340673.

[111] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to gps spoofing," *IEEE Trans. on Smart Grid*, vol. 10, no. 4, pp. 3535–3548, July 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8347144.

[112] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, Dec. 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8220480.

[113] L. Ponemon, "Calculating the cost of a data breach in 2018, the age of AI and the IoT," July 2018. [Online]. Available: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/.

[114] M. A. H. Kermani1, M. A. Golkar, and S. Zokaei, "Providing a model for a cyber-attack to a special protection scheme based on timed petri net," *Journal of Energy Management and Technology*, vol. 3, no. 2, pp. 22–33, April 2019.

[115] L. Teo, Y.-A. Sun, and G.-J. Ahn, "Defeating Internet attacks using risk awareness and active honeypots," in *Second IEEE International Information Assurance Workshop, 2004. Proceedings*, April 2004. [Online]. Available: https://ieeexplore.ieee.org/document/1288045.

[116] Working Group B5.19, "Protection relay coordination," CIGRE, Paris, Tech.

Rep. TB432, Oct. 2010. [Online]. Available: https://e-cigre.org/publication/432-protection-relay-coordination

[117] R. D. Christie, "Power systems test case archive," Aug. 1999. [Online]. Available: http://labs.ece.uw.edu/pstca/pf30/pg_tca30bus.htm.

[118] Bitdefender Labs, "New hide-and-seek IoT botnet using custom-built peer-to-peer communication spotted in the wild," Jan. 2018. [Online]. Available: https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/.

[119] Akamai, "Upnproxy: Blackhat proxies via NAT injections." [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf.

[120] Cisco Talos Intelligence Group, "New VPN filter malware targets at least 500k networking devices worldwide," May 2018. [Online]. Available: https://blog.talosintelligence.com/2018/05/VPNFilter.html.

[121] M. Corporation, "CVE details -security vulnerabilities (CVSS score between 9 and 10)." [Online]. Available: https://www.cvedetails.com/vulnerability-list/cvssscoremin-9/cvssscoremax-10/vulnerabilities.html.

[122] O. Security, "Exploit database." [Online]. Available: https://www.exploit-db.com/.

[123] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. V. Cutsem, and V. Vittal, "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Trans. on Power Syst.*, vol. 19, no. 3, pp. 1387–1401, 2004.

[124] Working Group C2.21, "Lessons learnt from recent emergencies and blackout incidents," CIGRE, Paris, Tech. Rep. TB608, Jan. 2015.

[125] Working Group C2/C4.37, "A proposed framework for coordinated power system stability control," CIGRE, Paris, Tech. Rep. TB742, Sep. 2018.

[126] U. G. Knight, *Power Systems in Emergencies: From Contingency Planning to Crisis Management*, 1st ed. Baffins Lane, Chichester, UK: Wiley, 2001.

[127] C.-W. Ten, K. Yamashita, Z. Yang, A. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4405–4425, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7827087.

[128] Z. Huang, Y. Chen, and J. Nieplocha, "Massive contingency analysis with high performance computing," in *Power Energy Society General Meeting, 2009. PES '09. IEEE*, Calgary, AB, July 2009, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/document/5275421

[129] V. Vittal, J. D. McCalley, P. Anderson, and A. Fouad, *Power System Control and Stability*, 3rd ed. Wiley-IEEE Press, Oct. 2019.

[130] P. Kundar, *Power System Stability and Control*, 1st ed. McGraw-Hill, Jan. 1994.

[131] *IEEE Recommended Practice for Excitation System Models for Power System Stability Studies*, IEEE, New York, NY, 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7553421

[132] H. Taniguchi, *Power System Analysis – Modeling and Simulation (Japanese)*, 1st ed. IEEJ and Ohmsha, Aug. 2009.

[133] P. Pourbeik, "Dynamic models for turbine-governors in power system studies," IEEE PES, Tech. Rep. PES-TR1, Jan. 2013.

[134] K. Yamashita, C.-W. Ten, and L. Wang, "Dynamical analysis of cyber-related contingencies initiated from substations," in *Security of Cyber-Physical Systems*, H. Karimipour, P. Srikantha, H. Farag, and J. Wei-Kocsis, Eds. Springer, Cham, 2020, pp. 223–246. [Online]. Available: https://doi.org/10.1007/978-3-030-45541-5_12.

[135] ERCOT, "ERCOT nodal operating guides – section 2: System operations and control requirements," May 2019. [Online]. Available: http://ercot.com/content/wcm/current_guides/53525/02-060119.doc.

[136] *PJM Manual 36: System Restoration Revision: 25*, PJM System Operations Division, June 2018. [Online]. Available: https://www.pjm.com/~/media/documents/manuals/m36.ashx.

[137] IEEE SCC 21 Standards Coordinating Committee on Fuel Cells Photovoltaics Dispersed Generation and Energy Storage, *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*. IEEE, April 2018.

[138] J. L. Blackburn and T. J. Domin, *Protective relaying: principles and applications*, 4th ed. CRC press, 2014.

[139] *IEEE Standard for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations*, IEEE, New York, NY, 2008. [Online]. Available: https://ieeexplore.ieee.org/document/4639522

[140] Working Group C4.605, "Modeling and aggregation of loads in flexible power networks," CIGRE, Paris, Tech. Rep. TB566, Feb. 2014. [Online]. Available: https://e-cigre.org/publication/566-modelling-and-aggregation-of-loads-in-flexible-power-networks

[141] J. V. Milanovic, K. Yamashita, S. M. Villanueva, S. Z. Djokic, and L. M. Korunovic, "International industry practice on power system load modeling," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3038–12, Aug. 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6399552

[142] S. M. Villanueva, K. Yamashita, L. M. Korunovic, S. Z. Djokic, J. Matevosyan, A. Borghetti, Z. Y. Dong, and J. V. Milanovic, "CIGRE WG C4.605 – modeling and aggregation of loads in flexible power networks – scope and status of the work by june 2012," in *Proc. of CIGRE C4 Colloquium*, Hakodate, Japan, 2012, pp. 109–114.

[143] Y. Tang, S. Zhao, C. Ten, K. Zhang, and L. Thillainathan, "Establishment of enhanced load modeling by correlating with occupancy information," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1702–1713, March 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8844854

[144] K. Yamashita, S. Z. Djokic, F. Villella, and J. V. Milanovic, "Self-disconnection and self-recovery of loads due to voltage sags and short interruptions," in *Proc. of CIGRE Symposium*, Lisbon, Portugal, April 2013, pp. 22–24.

[145] Power System Stability Study Group, "Integrated analysis software for bulk power system stability," CRIEPI, Tech. Rep. ET90002, July 1991.

[146] M. J. Eppstein and P. D. H. Hines, "A "random chemistry" algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1698–1705, Aug. 2012. [Online]. Available: https://ieeexplore.ieee.org/document/6152191.

[147] Q. Chen and J. McCalley, "Identifying high risk n-k contingencies for on-line

secrity assessment," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 823–834, May 2005. [Online]. Available: https://ieeexplore.ieee.org/document/1425578

[148] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with DC power flow model and transient stability analysis," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 285–297, Jan. 2015. [Online]. Available: https://ieeexplore.ieee.org/document/6819069.

[149] M. Rios, K. Bell, D. Kirschen, and R. Allan. (1999) Computation of the value of security. Manchester Centre for Electrical Energy, UMIST. [Online]. Available: http://www2.ee.washington.edu/research/real/Library/Reports/Value_of_Security_Part_I.pdf.

[150] P. Rezaei. (2015) Cascading failure risk estimation and mitigation in power systems. University of Vermont. [Online]. Available: https://core.ac.uk/download/pdf/51067213.pdf.

[151] R. Sun, Z. Wu, and V. A. Centeno, "Power system islanding detection & identification using topology approach and decision tree," in *Power and Energy Society General Meeting, 2011 IEEE*, San Diego, CA, July 2011, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/6039088.

[152] L. Ding, F. M. Gonzalez-Longatt, P. Wall, and V. Terzija, "Two-step spectral clustering controlled islanding algorithm," *IEEE Trans.*

Power Syst., vol. 28, no. 1, pp. 75–84, Feb. 2013. [Online]. Available: https://ieeexplore.ieee.org/document/6213172.

[153] V. Liudmyla. (2013, July) Power system of ukrine: today and tomorrow. [Online]. Available: https://eneken.ieej.or.jp/data/5026.pdf.

[154] Ukrenergo. Grid -composition of the trunk and interstate power grid of ukrenergo. [Online]. Available: https://ua.energy/transmission-and-dispatching/networks/.

Appendix A

Reuse Permission

The dissertation has obtained the reuse permissions from The Institute of Electrical and Electronics Engineers, Inc. Copyright © 2020 IEEE and Copyright © 2020, Springer Nature Switzerland AG.

© 2020 IEEE. Reprinted, with permission, from Koji Yamashita, Chee-Wooi Ten, Yeonwoo Rho, Lingfeng Wang, Wei Wei and Andrew Francis Ginter, Measuring Systemic Risk of Switching Attacks Based on Cybersecurity Technologies in Substations, IEEE Transactions on Power Systems, November 2020.

© 2018 IEEE. Reprinted, with permission, from Chee-Wooi Ten, Koji Yamashita, Zhiyuan Yang, Athanasios V. Vasilakos, and Andrew Ginter, Impact assessment of hypothesized cyberattacks on interconnected bulk power systems, IEEE Transactions

on Smart Grid, September 2018.

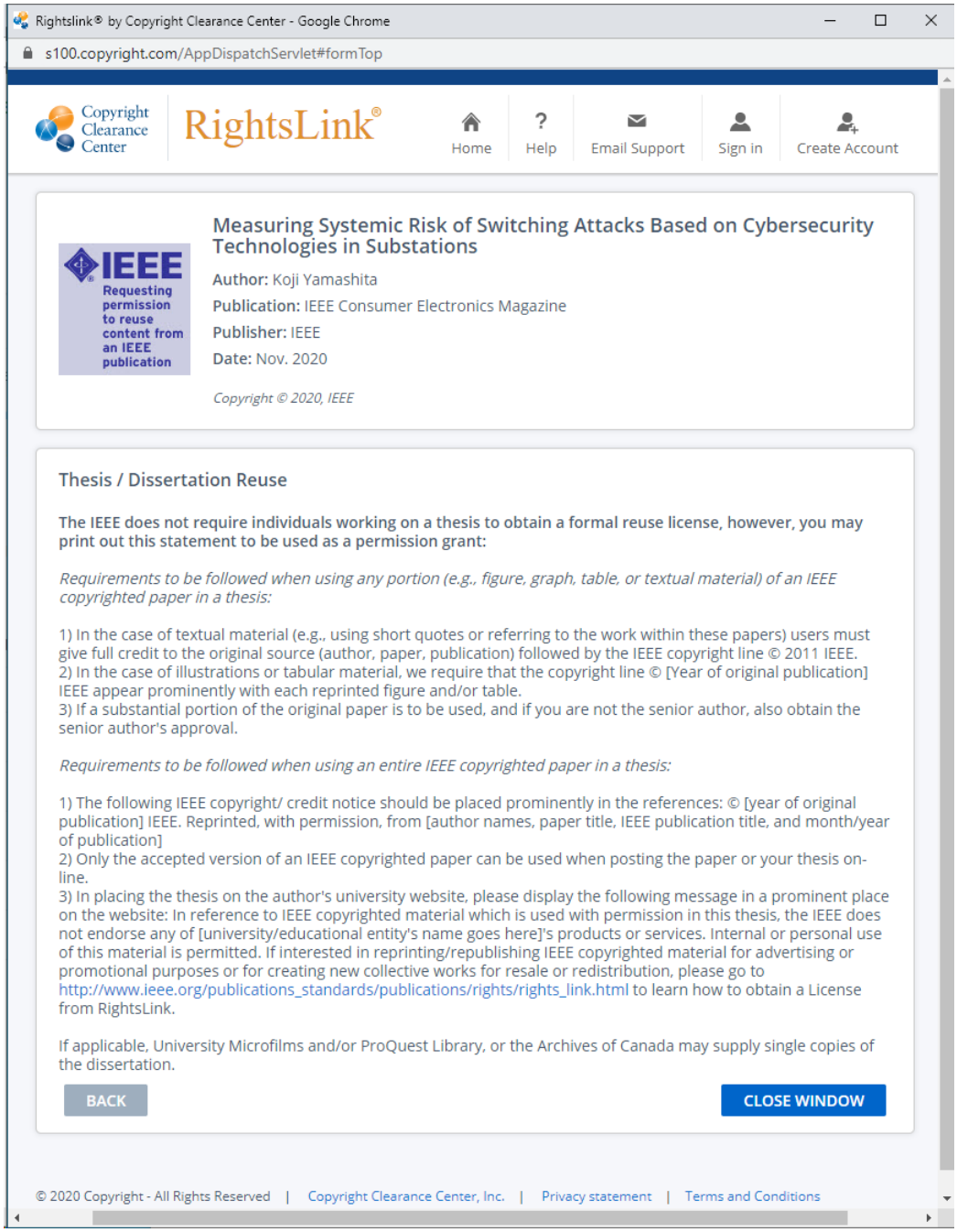


Figure A.1: Reuse permission of the first paper obtained from IEEE copyright center

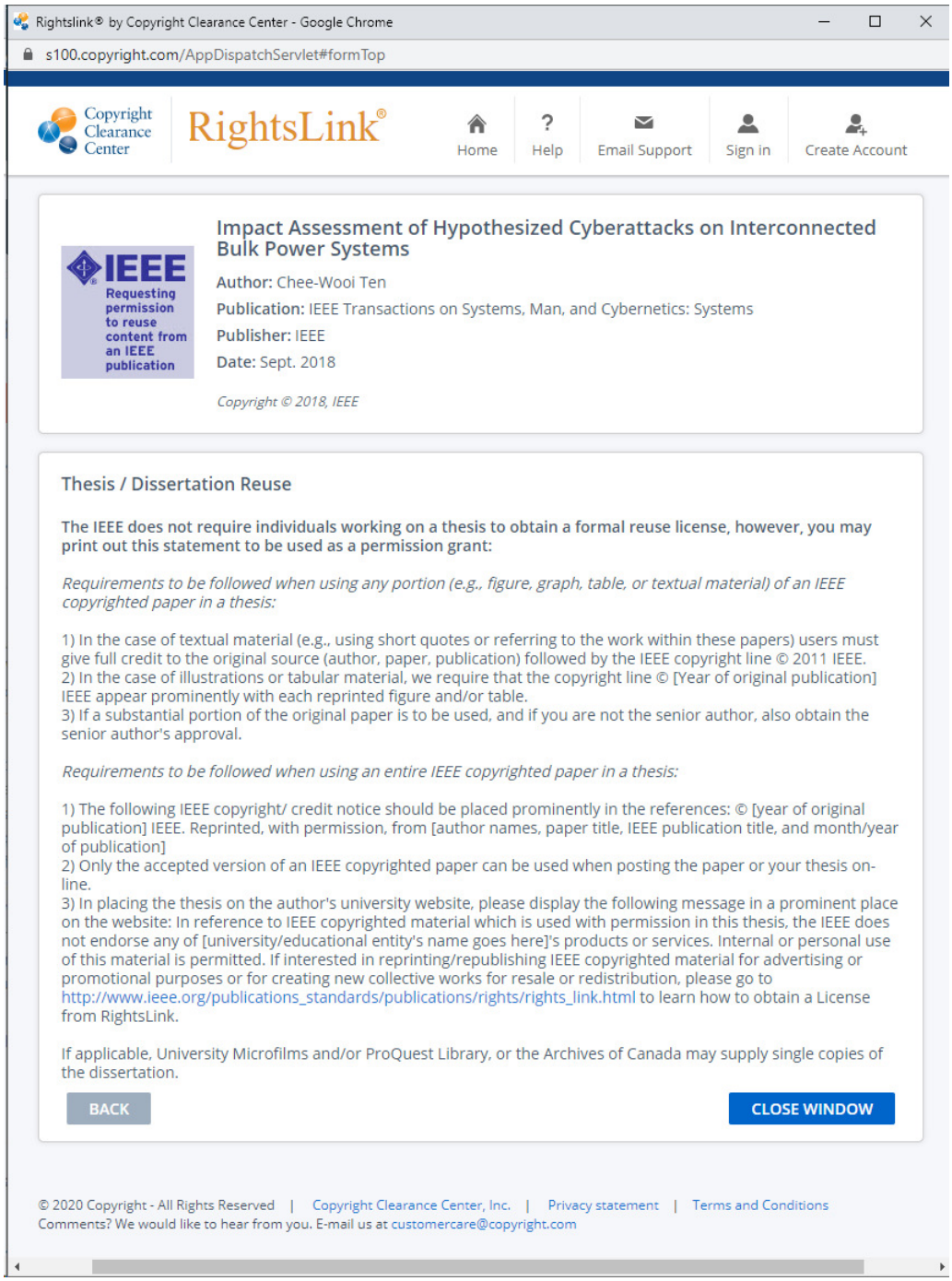


Figure A.2: Reuse permission of the second paper obtained from IEEE copyright center

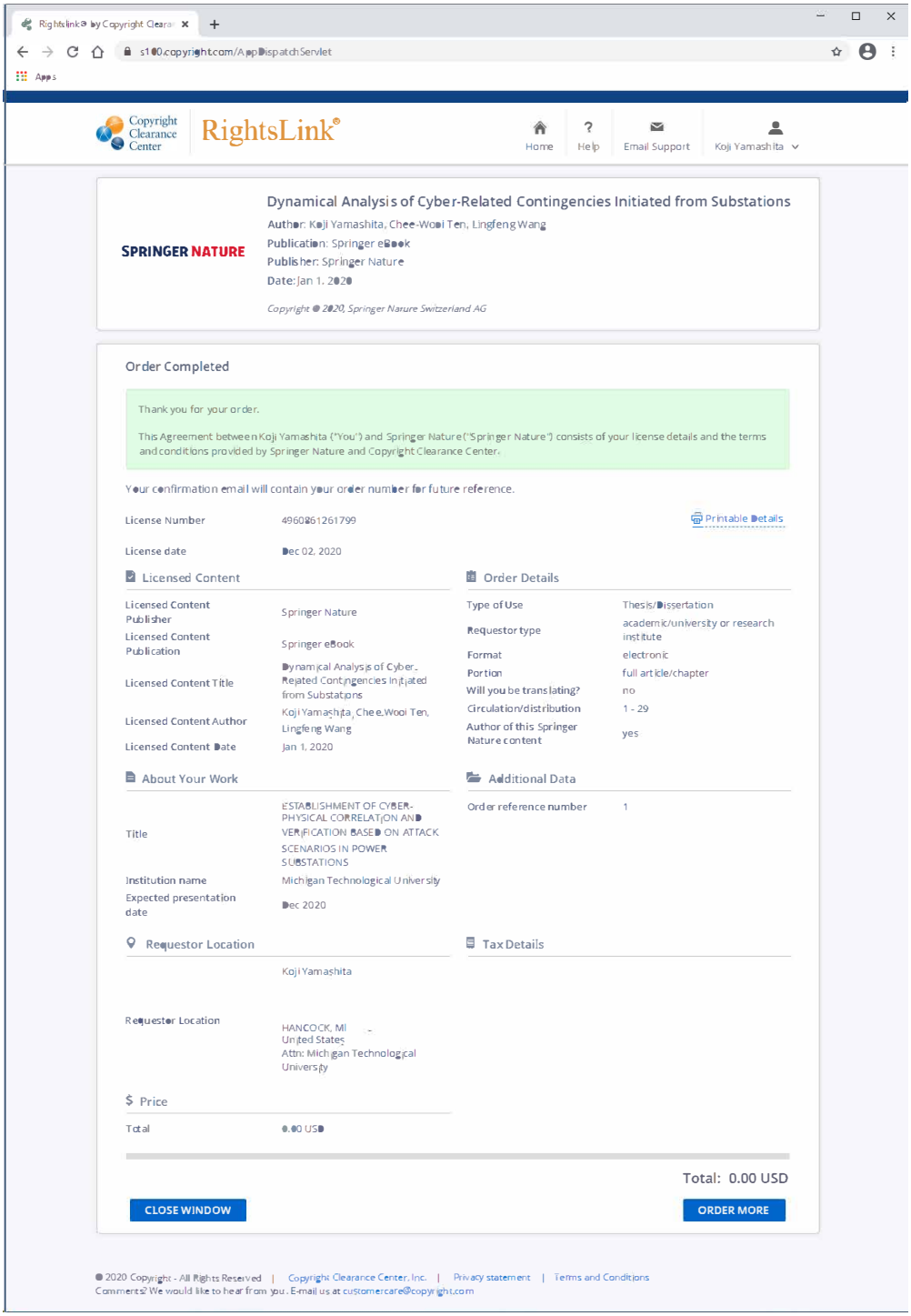


Figure A.3: Reuse permission of the book chapter obtained from Springer Nature copyright center

Appendix B

Power Flow Solution and Initial Condition of Dynamic Simulation in IEEE standard models

B.1 IEEE 14-bus System

The system diagram is shown in Fig. B.1. Power flow solutions are summarized in Tables B.1 and B.2. The system MVA is 100 MVA. The power flow setting data are also provided in Tables B.3 and B.4. It is noted that circuit breakers with no impedance are inserted between the main grid and individual power equipment.

Initial conditions of the dynamic simulation with generator constants are sorted out in Tables B.5, B.6 and B.7. It is noted that the inertia constant of synchronous condensers is set at 25% of synchronous generators, assuming that the generator per se shares 25% of the whole unit that comprises turbines and generators.

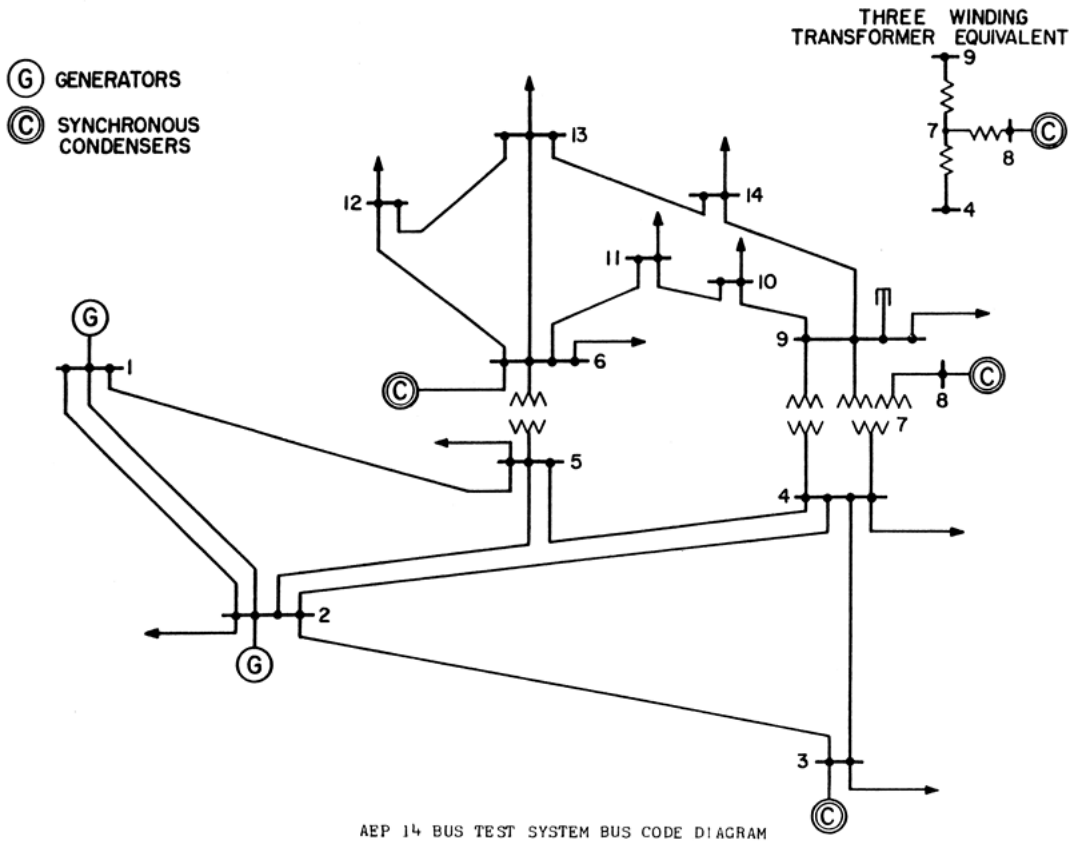


Figure B.1: IEEE 14-bus system diagram

Table B.1
Power flow node solution in IEEE 14-bus system

Node	Voltage magnitude (p.u.)	Voltage angle (deg)	PG (p.u.)	QG (p.u.)	PL (p.u.)	QL (p.u.)	QC (p.u.)	Name
1	1.0600	0.00	0.7736	-0.0500	0.0000	0.0000	0.0000	SWING
2	1.0450	-4.98	0.4000	0.4355	0.0000	0.0000	0.0000	G02
3	1.0100	-12.71	0.0000	0.0000	0.9420	0.1900	0.0000	L03
4	1.0177	-10.30	0.0000	0.0000	0.4780	-0.0390	0.0000	L04
5	1.0196	-8.76	0.0000	0.0000	0.0760	0.0160	0.0000	L05
6	1.0700	-14.21	0.0000	0.0000	0.1120	0.0750	0.0000	L06
7	1.0615	-13.35	0.0000	0.0000	0.0000	0.0000	0.0000	
8	1.0900	-13.35	0.0000	0.0000	0.0000	0.0000	0.0000	
9	1.0560	-14.93	0.0000	0.0000	0.2950	0.1660	0.2119	L09
10	1.0510	-15.08	0.0000	0.0000	0.0900	0.0580	0.0000	L10
11	1.0569	-14.78	0.0000	0.0000	0.0350	0.0180	0.0000	L11
12	1.0552	-15.06	0.0000	0.0000	0.0610	0.0160	0.0000	L12
13	1.0504	-15.14	0.0000	0.0000	0.1350	0.0580	0.0000	L13
14	1.0355	-16.02	0.0000	0.0000	0.1490	0.0500	0.0000	L14
15	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
16	1.0450	-4.98	0.0000	0.0000	0.2170	0.1270	0.0000	G02
21	1.0600	0.00	0.7750	-0.0575	0.0000	0.0000	0.0000	SWING_B
23	1.0100	-12.71	0.0000	0.2499	0.0000	0.0000	0.0000	C02
26	1.0700	-14.21	0.0000	0.1269	0.0000	0.0000	0.0000	C06
28	1.0900	-13.35	0.0000	0.1761	0.0000	0.0000	0.0000	C08
31	1.0600	0.00	0.7750	-0.0572	0.0000	0.0000	0.0000	SWING_C
44	1.0177	-10.30	0.0000	0.0000	0.0000	0.0000	0.0000	
45	1.0196	-8.76	0.0000	0.0000	0.0000	0.0000	0.0000	
46	1.0700	-14.21	0.0000	0.0000	0.0000	0.0000	0.0000	
49	1.0560	-14.93	0.0000	0.0000	0.0000	0.0000	0.0000	
51	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
61	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
71	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
80	1.0450	-4.98	0.0000	0.0000	0.0000	0.0000	0.0000	
93	1.0100	-12.71	0.0000	0.0000	0.0000	0.0000	0.0000	
96	1.0700	-14.21	0.0000	0.0000	0.0000	0.0000	0.0000	
98	1.0900	-13.35	0.0000	0.0000	0.0000	0.0000	0.0000	
Total			2.7237	0.8236	2.5900	0.7350	0.2119	

Table B.2
Power flow branch solution in IEEE 14-bus system

From	To	Psend (p.u.)	Qsend (p.u.)	Prec (p.u.)	Qrec (p.u.)	Ploss (p.u.)	Qloss (p.u.)
15	16	1.5682	-0.2035	1.5253	-0.2761	0.0429	0.0725
15	5	0.7554	0.0388	0.7279	-0.0219	0.0276	0.0607
16	3	0.7324	0.0360	0.7093	-0.0155	0.0232	0.0515
16	4	0.5611	-0.0154	0.5444	-0.0300	0.0167	0.0146
16	5	0.4148	0.0118	0.4058	0.0212	0.0090	-0.0094
3	4	0.2327	0.0444	-0.2365	0.0480	0.0037	-0.0036
4	5	0.6116	0.1580	-0.6168	0.1418	0.0051	0.0162
6	11	0.0735	0.0356	0.0730	0.0344	0.0006	0.0012
6	12	0.0779	0.0250	0.0771	0.0235	0.0007	0.0015
6	13	0.1775	0.0721	0.1754	0.0680	0.0021	0.0042
7	8	0.0000	-0.1715	0.0000	-0.1761	0.0000	0.0046
7	9	0.2807	0.0578	0.2807	0.0498	0.0000	0.0080
9	10	0.0523	0.0422	0.0522	0.0419	0.0001	0.0003
9	14	0.0943	0.0361	0.0931	0.0337	0.0012	0.0025
10	11	0.0378	-0.0161	-0.0380	-0.0164	0.0001	0.0003
12	13	0.0161	0.0075	0.0161	0.0075	0.0001	0.0001
13	14	0.0564	0.0174	0.0559	0.0163	0.0005	0.0011
4	7	0.2807	-0.0967	0.2807	-0.1137	0.0000	0.0170
44	49	0.1608	-0.0042	0.1608	-0.0173	0.0000	0.0130
45	46	0.4409	0.1251	0.4409	0.0809	0.0000	0.0442

The total P loss and Q loss are 0.1337 (p.u.) and 0.3005 (p.u.), individually.

Table B.3
System (branch) setting data

From	To	Resistance	Reactance	Capacitance (Y/2)	Tap	Remark
15	16	0.01938	0.05917	0.02640	0.00000	
15	5	0.05403	0.22304	0.02460	0.00000	
16	3	0.04699	0.19797	0.02190	0.00000	
16	4	0.05811	0.17632	0.01700	0.00000	
16	5	0.05695	0.17388	0.01730	0.00000	
3	4	0.06701	0.17103	0.00640	0.00000	
4	5	0.01335	0.04211	0.00000	0.00000	
6	11	0.09498	0.19890	0.00000	0.00000	
6	12	0.12291	0.25581	0.00000	0.00000	
6	13	0.06615	0.13027	0.00000	0.00000	
7	8	0.00000	0.17615	0.00000	0.00000	
7	9	0.00000	0.11001	0.00000	0.00000	
9	10	0.03181	0.08450	0.00000	0.00000	
9	14	0.12711	0.27038	0.00000	0.00000	
10	11	0.08205	0.19207	0.00000	0.00000	
12	13	0.22092	0.19988	0.00000	0.00000	
13	14	0.17093	0.34802	0.00000	0.00000	
4	7	0.00000	0.20912	0.00000	1.02250	
44	49	0.00000	0.55618	0.00000	1.03200	
45	46	0.00000	0.25202	0.00000	1.07300	
4	44	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
9	49	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
5	45	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
6	46	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
1	51	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
51	15	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
21	61	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
61	15	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
31	71	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
71	15	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
2	80	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
80	16	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
23	93	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
93	3	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
26	96	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
96	6	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
28	98	0.00000	0.00000	0.00000	0.00000	Circuit Breaker
98	8	0.00000	0.00000	0.00000	0.00000	Circuit Breaker

Table B.4
Power flow condition setting data

Node	Voltage magnitude	PG	QG	PL	QL	YC	Name
1	1.0600	0.0000	0.0000	0.0000	0.0000	0.0000	SWING-A
2	1.0450	0.4000	0.0000	0.0000	0.0000	0.0000	G02
3	0.0000	0.0000	0.0000	0.9420	0.1900	0.0000	L03
4	0.0000	0.0000	0.0000	0.4780	-0.0390	0.0000	L04
5	0.0000	0.0000	0.0000	0.0760	0.0160	0.0000	L05
6	0.0000	0.0000	0.0000	0.1120	0.0750	0.0000	L06
7	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
8	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
9	0.0000	0.0000	0.0000	0.2950	0.1660	0.1900	L09
10	0.0000	0.0000	0.0000	0.0900	0.0580	0.0000	L10
11	0.0000	0.0000	0.0000	0.0350	0.0180	0.0000	L11
12	0.0000	0.0000	0.0000	0.0610	0.0160	0.0000	L12
13	0.0000	0.0000	0.0000	0.1350	0.0580	0.0000	L13
14	0.0000	0.0000	0.0000	0.1490	0.0500	0.0000	L14
15	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
16	0.0000	0.0000	0.0000	0.2170	0.1270	0.0000	G02
21	1.0600	0.7750	0.0000	0.0000	0.0000	0.0000	SWING-B
23	1.0100	0.0000	0.0000	0.0000	0.0000	0.0000	C02
26	1.0700	0.0000	0.0000	0.0000	0.0000	0.0000	C06
28	1.0900	0.0000	0.0000	0.0000	0.0000	0.0000	C08
31	1.0600	0.7750	0.0000	0.0000	0.0000	0.0000	SWING-C
44	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
45	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
46	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
49	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
51	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
61	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
71	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
80	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
93	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
96	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
98	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.5
Generator constants with implemented generator controller

Bus	AVR	OEL	PSS	GOV	GMVA	GMW	GPF	MG (s)	DG	PLM (%)	NAME
1	✓	✓		✓	100.0	85.0	0.85	6.00	0.0	5.00	Generator 1-A
21	✓	✓		✓	100.0	85.0	0.85	6.00	0.0	5.00	Generator 1-B
31	✓	✓		✓	100.0	85.0	0.85	6.00	0.0	5.00	Generator 1-C
2	✓	✓		✓	60.0	48.0	0.80	6.00	0.0	5.00	Generator 2
23	✓				60.0	0.0	0.00	1.50	0.0	0.00	Condenser 3
26	✓				25.0	0.0	0.00	1.50	0.0	0.00	Condenser 6
28	✓				25.0	0.0	0.00	1.50	0.0	0.00	Condenser 8

Table B.6
Generator constants of the used generator model

Bus	RA	XL	XD	XDD	XDDD	XFLD	XKLD	XQ	XQDD	XKLQ	TDD	TDDD	RFD	RKD	TQDD	RKQ
1	.0017	.2250	1.700	0.350	0.250	.1366	.0312	1.700	0.250	.0254	1.000	0.030	.0009	.0099	0.030	.0195
21	.0017	.2250	1.700	0.350	0.250	.1366	.0312	1.700	0.250	.0254	1.000	0.030	.0009	.0099	0.030	.0195
31	.0017	.2250	1.700	0.350	0.250	.1366	.0312	1.700	0.250	.0254	1.000	0.030	.0009	.0099	0.030	.0195
2	.0017	.2250	1.700	0.350	0.250	.1366	.0312	1.700	0.250	.0254	1.000	0.030	.0009	.0099	0.030	.0195
23	.0017	.2250	1.700	0.350	0.250	.1366	.0312	1.700	0.250	.0254	1.000	0.030	.0009	.0099	0.030	.0195
26	.0017	.2250	1.700	0.350	0.250	.1366	.0312	1.700	0.250	.0254	1.000	0.030	.0009	.0099	0.030	.0195
28	.0017	.2250	1.700	0.350	0.250	.1366	.0312	1.700	0.250	.0254	1.000	0.030	.0009	.0099	0.030	.0195

Note:

RA: Armature resistance (p.u.)

XL: Leakage reactance (p.u.)

XD: D-axis reactance (p.u.)

XDD: D-axis transient reactance (p.u.)

XDDD: D-axis sub-transient reactance (p.u.)

XFLD: D-axis field circuit reactance (p.u.)

XKLD: D-axis damper circuit reactance (p.u.)

XQ: Q-axis reactance (p.u.)

XQD: Q-axis transient reactance (p.u.)

XQDD: Q-axis sub-transient reactance (p.u.)

XFLQ: Q-axis field circuit reactance (p.u.)

XKLQ: Q-axis damper circuit reactance (p.u.)

TDD: D-axis transient time constant [s]

TDDD: D-axis sub-transient time constant [s]

RFD: D-axis field circuit resistance (p.u.)

RKD: D-axis damper circuit resistance (p.u.)

TDDD: Q-axis sub-transient time constant [s]

RKQ: Q-axis damper circuit resistance (p.u.)

Table B.7
Initial condition of synchronous generator and synchronous condenser

Bus	AGG	VT	PG	QG	TQG	EF	CF	CDD	CQQ	FGD	FGQ
1	51.89	1.0600	0.7736	-0.0549	0.7745	1.5769	1.5769	0.5423	0.4912	0.7770	-0.7245
21	51.94	1.0600	0.7750	-0.0549	0.7759	1.5786	1.5786	0.5438	0.4915	0.7766	-0.7250
31	51.94	1.0600	0.7750	-0.0549	0.7759	1.5787	1.5787	0.5438	0.4915	0.7766	-0.7249
2	20.97	1.0450	0.6667	0.7258	0.6681	2.4764	2.4764	0.9037	0.2698	1.1435	-0.3980
23	-12.73	1.0100	0.0000	0.4164	0.0003	1.7109	1.7109	0.4123	0.0002	1.1028	-0.0003
26	-14.23	1.0700	0.0000	0.5074	0.0004	1.8762	1.8762	0.4742	0.0002	1.1767	-0.0003
28	-13.37	1.0900	0.0000	0.7044	0.0007	2.1887	2.1887	0.6463	0.0003	1.2354	-0.0005

Note:

BUS: Node number which the designated generator is connected

AGG: Rotor angle of generator with relative to the center of angle (deg)

VT: Terminal voltage (p.u.)

PG: Active power output (Machine base p.u.)

QG: Reactive power output (Machine base p.u.)

TQG: Turbine output (Machine base p.u.)

EF: Field voltage (p.u.)

CF: Field current (p.u.)

CDD: D-axis armature current (p.u.)

CQQ: Q-axis armature current (p.u.)

FGD: D-axis interlinkage magnetic flux (p.u.)

FGQ: Q-axis interlinkage magnetic flux (p.u.)

B.2 IEEE 30-bus System

The system diagram is shown in Fig. B.2. Power flow solutions are summarized in Tables B.8, B.9, B.10, B.11, and B.12. The system MVA is 100 MVA. The power flow setting data are also provided in Tables B.13, B.14, B.15, B.16 and B.17. It is noted that circuit breakers with no impedance are inserted between the main grid and individual power equipment.

Initial conditions of the dynamic simulation with generator constants are sorted out in Tables B.18, B.19 and B.20.

It is noted that the generator's saturation characteristics is used for the IEEE 30-bus systems (Fig. B.3). We may use this characteristic for the IEEE 14-bus system, although it is skipped for the IEEE 14-bus system.

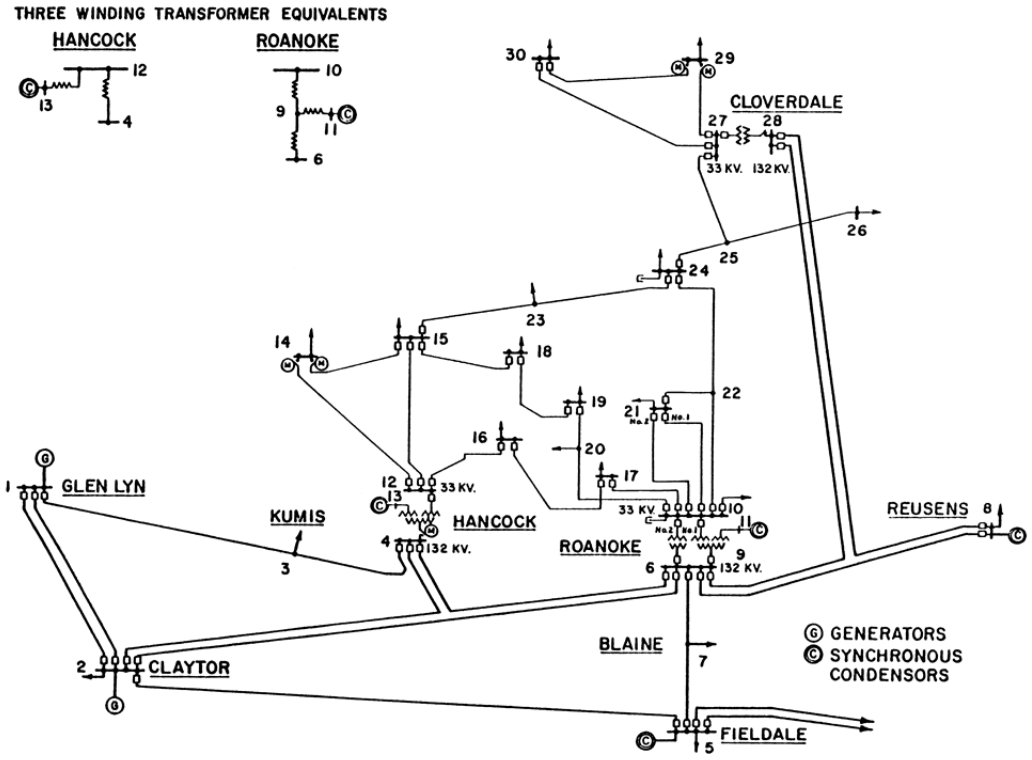


Figure B.2: IEEE 30-bus system diagram

Table B.8
Power flow node solution in IEEE 30-bus system (part 1)

Node	V magnitude (p.u.)	V angle (deg)	PG (p.u.)	QG (p.u.)	PL (p.u.)	QL (p.u.)	QC (p.u.)	Name
1	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	Glen LynA1
2	1.0430	-5.35	0.0000	0.0000	0.2170	0.1270	0.0000	Claytor1
3	1.0206	-7.52	0.0000	0.0000	0.0240	0.0120	0.0000	Kumis
4	1.0116	-9.27	0.0000	0.0000	0.0760	0.0160	0.0000	Hancock
5	1.0100	-14.15	0.0000	0.0000	0.9420	0.1900	0.0000	Fieldale1
6	1.0100	-11.05	0.0000	0.0000	0.0000	0.0000	0.0000	Roanoke
7	1.0022	-12.85	0.0000	0.0000	0.2280	0.1090	0.0000	Blaine
8	1.0100	-11.80	0.0000	0.0000	0.3000	0.3000	0.0000	Reusens1
9	1.0499	-14.09	0.0000	0.0000	0.0000	0.0000	0.0000	1kVRoanoke
10	1.0431	-15.68	0.0000	0.0000	0.0580	0.0200	0.1893	33kVRoanoke
11	1.0820	-14.09	0.0000	0.0000	0.0000	0.0000	0.0000	11kVRoanoke1
12	1.0565	-14.95	0.0000	0.0000	0.1120	0.0750	0.0000	33kVHancock
13	1.0710	-14.95	0.0000	0.0000	0.0000	0.0000	0.0000	11kVHancock1
14	1.0415	-15.84	0.0000	0.0000	0.0620	0.0160	0.0000	33kVBus_14
15	1.0367	-15.93	0.0000	0.0000	0.0820	0.0250	0.0000	33kVBus_15
16	1.0432	-15.52	0.0000	0.0000	0.0350	0.0180	0.0000	33kVBus_16
17	1.0381	-15.85	0.0000	0.0000	0.0900	0.0580	0.0000	33kVBus_17
18	1.0268	-16.54	0.0000	0.0000	0.0320	0.0090	0.0000	33kVBus_18
19	1.0241	-16.71	0.0000	0.0000	0.0950	0.0340	0.0000	33kVBus_19
20	1.0280	-16.51	0.0000	0.0000	0.0220	0.0070	0.0000	33kVBus_20
21	1.0307	-16.13	0.0000	0.0000	0.1750	0.1120	0.0000	33kVBus_21
22	1.0313	-16.11	0.0000	0.0000	0.0000	0.0000	0.0000	33kVBus_22
23	1.0259	-16.31	0.0000	0.0000	0.0320	0.0160	0.0000	33kVBus_23
24	1.0198	-16.48	0.0000	0.0000	0.0870	0.0670	0.0429	33kVBus_24
25	1.0161	-16.06	0.0000	0.0000	0.0000	0.0000	0.0000	33kVBus_25
26	0.9984	-16.48	0.0000	0.0000	0.0350	0.0230	0.0000	33kVBus_26
27	1.0224	-15.54	0.0000	0.0000	0.0000	0.0000	0.0000	33kCloverdle
28	1.0066	-11.68	0.0000	0.0000	0.0000	0.0000	0.0000	Cloverdle
29	1.0025	-16.77	0.0000	0.0000	0.0240	0.0090	0.0000	33kVBus_29
30	0.9910	-17.66	0.0000	0.0000	0.1060	0.0190	0.0000	33kVBus_30
36	1.0100	-11.05	0.0000	0.0000	0.0000	0.0000	0.0000	
39	1.0499	-14.09	0.0000	0.0000	0.0000	0.0000	0.0000	
40	1.0431	-15.68	0.0000	0.0000	0.0000	0.0000	0.0000	
44	1.0116	-9.27	0.0000	0.0000	0.0000	0.0000	0.0000	
47	1.0224	-15.54	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.9
Power flow node solution in IEEE 30-bus system (Part 2)

Node	V magnitude (p.u.)	V angle (deg)	PG (p.u.)	QG (p.u.)	PL (p.u.)	QL (p.u.)	QC (p.u.)	Name
48	1.0066	-11.68	0.0000	0.0000	0.0000	0.0000	0.0000	
52	1.0565	-14.95	0.0000	0.0000	0.0000	0.0000	0.0000	
56	1.0100	-11.05	0.0000	0.0000	0.0000	0.0000	0.0000	
201	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
202	1.0430	-5.35	0.0000	0.0000	0.0000	0.0000	0.0000	
205	1.0100	-14.15	0.0000	0.0000	0.0000	0.0000	0.0000	
208	1.0100	-11.80	0.0000	0.0000	0.0000	0.0000	0.0000	
211	1.0820	-14.09	0.0000	0.0000	0.0000	0.0000	0.0000	
213	1.0710	-14.95	0.0000	0.0000	0.0000	0.0000	0.0000	
271	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
281	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
301	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
302	1.0430	-5.35	0.0000	0.0000	0.0000	0.0000	0.0000	
305	1.0100	-14.15	0.0000	0.0000	0.0000	0.0000	0.0000	
308	1.0100	-11.80	0.0000	0.0000	0.0000	0.0000	0.0000	
311	1.0820	-14.09	0.0000	0.0000	0.0000	0.0000	0.0000	
313	1.0710	-14.95	0.0000	0.0000	0.0000	0.0000	0.0000	
371	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
381	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
401	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
402	1.0430	-5.35	0.0000	0.0000	0.0000	0.0000	0.0000	
405	1.0100	-14.15	0.0000	0.0000	0.0000	0.0000	0.0000	
408	1.0100	-11.80	0.0000	0.0000	0.0000	0.0000	0.0000	
411	1.0820	-14.09	0.0000	0.0000	0.0000	0.0000	0.0000	
413	1.0710	-14.95	0.0000	0.0000	0.0000	0.0000	0.0000	
471	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
481	1.0600	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
501	1.0600	0.00	0.8699	-0.0546	0.0000	0.0000	0.0000	Glen LynA2
502	1.0430	-5.35	0.4000	0.4984	0.0000	0.0000	0.0000	Claytor2
505	1.0100	-14.15	0.0000	0.3697	0.0000	0.0000	0.0000	Fieldale2
508	1.0100	-11.80	0.0000	0.3780	0.0000	0.0000	0.0000	Reusens2
511	1.0820	-14.09	0.0000	0.1671	0.0000	0.0000	0.0000	11kVRoanoke2
513	1.0710	-14.95	0.0000	0.1109	0.0000	0.0000	0.0000	11kVHancock2
571	1.0600	0.00	0.8698	-0.0545	0.0000	0.0000	0.0000	Glen LynB2
581	1.0600	0.00	0.8698	-0.0545	0.0000	0.0000	0.0000	Glen LynC2
Total			3.0094	1.3605	2.8340	1.2620	0.2322	

Table B.10
Power flow branch solution in IEEE 30-bus system (Part 1)

From	To	Psend (p.u.)	Qsend (p.u.)	Prec (p.u.)	Qrec (p.u.)	Ploss (p.u.)	Qloss (p.u.)
1	2	1.7322	-0.2105	1.6804	-0.3073	0.0518	0.0968
1	3	0.8772	0.0469	0.8461	-0.0226	0.0311	0.0695
2	4	0.4361	0.0403	0.4259	0.0483	0.0101	-0.0079
3	4	0.8221	-0.0346	0.8135	-0.0506	0.0086	0.0160
2	5	0.8241	0.0179	0.7946	-0.0619	0.0295	0.0798
2	6	0.6032	0.0059	0.5838	-0.0137	0.0194	0.0196
4	6	0.7206	-0.1628	0.7142	-0.1756	0.0063	0.0128
5	7	-0.1474	0.1178	-0.1491	0.1341	0.0017	-0.0163
6	7	0.3809	-0.0306	0.3771	-0.0251	0.0038	-0.0055
6	8	0.2958	-0.0861	0.2947	-0.0808	0.0011	-0.0053
9	11	0.0000	-0.1621	0.0000	-0.1671	0.0000	0.0050
9	10	0.2765	0.0684	0.2765	0.0603	0.0000	0.0081
12	13	0.0000	-0.1094	0.0000	-0.1109	0.0000	0.0015
12	14	0.0788	0.0247	0.0781	0.0231	0.0008	0.0016
12	15	0.1794	0.0705	0.1772	0.0662	0.0022	0.0043
12	16	0.0727	0.0365	0.0722	0.0354	0.0006	0.0012
14	15	0.0161	0.0071	0.0160	0.0070	0.0001	0.0001
16	17	0.0372	0.0174	0.0371	0.0171	0.0001	0.0003
15	18	0.0605	0.0176	0.0601	0.0168	0.0004	0.0008
18	19	0.0281	0.0078	0.0281	0.0077	0.0001	0.0001
19	20	-0.0669	-0.0263	-0.0671	-0.0267	0.0002	0.0003
10	20	0.0899	0.0355	0.0891	0.0337	0.0008	0.0018
10	17	0.0530	0.0413	0.0529	0.0409	0.0001	0.0004
10	21	0.1575	0.0995	0.1564	0.0971	0.0011	0.0024
10	22	0.0760	0.0456	0.0754	0.0445	0.0005	0.0011
21	22	-0.0186	-0.0149	-0.0186	-0.0149	0.0000	0.0000
15	23	0.0506	0.0307	0.0503	0.0300	0.0003	0.0007
22	24	0.0568	0.0296	0.0564	0.0289	0.0004	0.0007
23	24	0.0183	0.0140	0.0182	0.0139	0.0001	0.0001
24	25	-0.0124	0.0187	-0.0125	0.0185	0.0001	0.0002
25	26	0.0354	0.0237	0.0350	0.0230	0.0004	0.0007
25	27	-0.0479	-0.0052	-0.0482	-0.0056	0.0002	0.0005
27	29	0.0619	0.0167	0.0610	0.0151	0.0009	0.0016
27	30	0.0709	0.0166	0.0693	0.0136	0.0016	0.0031
29	30	0.0370	0.0061	0.0367	0.0054	0.0003	0.0006
8	28	-0.0053	-0.0028	-0.0054	0.0407	0.0000	-0.0435

Table B.11
Power flow branch solution in IEEE 30-bus system (Part 2)

From	To	Psend (p.u.)	Qsend (p.u.)	Prec (p.u.)	Qrec (p.u.)	Ploss (p.u.)	Qloss (p.u.)
6	28	0.1869	0.0001	0.1863	0.0113	0.0006	-0.0112
36	39	0.2765	-0.0776	0.2765	-0.0937	0.0000	0.0161
56	40	0.1579	0.0050	0.1579	-0.0078	0.0000	0.0128
44	52	0.4429	0.1445	0.4429	0.0973	0.0000	0.0472
48	47	0.1810	0.0519	0.1810	0.0390	0.0000	0.0130
6	36	0.2765	-0.0776	0.2765	-0.0776	0.0000	0.0000
39	9	0.2765	-0.0937	0.2765	-0.0937	0.0000	0.0000
6	56	0.1579	0.0050	0.1579	0.0050	0.0000	0.0000
40	10	0.1579	-0.0078	0.1579	-0.0078	0.0000	0.0000
4	44	0.4429	0.1445	0.4429	0.1445	0.0000	0.0000
52	12	0.4429	0.0973	0.4429	0.0973	0.0000	0.0000
28	48	0.1810	0.0519	0.1810	0.0519	0.0000	0.0000
47	27	0.1810	0.0390	0.1810	0.0390	0.0000	0.0000
1	201	-0.8699	0.0546	-0.8699	0.0546	0.0000	0.0000
201	301	-0.8699	0.0546	-0.8699	0.0546	0.0000	0.0000
301	401	-0.8699	0.0546	-0.8699	0.0546	0.0000	0.0000
401	501	-0.8699	0.0546	-0.8699	0.0546	0.0000	0.0000
1	271	-0.8698	0.0545	-0.8698	0.0545	0.0000	0.0000
271	371	-0.8698	0.0545	-0.8698	0.0545	0.0000	0.0000
371	471	-0.8698	0.0545	-0.8698	0.0545	0.0000	0.0000
471	571	-0.8698	0.0545	-0.8698	0.0545	0.0000	0.0000
1	281	-0.8698	0.0545	-0.8698	0.0545	0.0000	0.0000
281	381	-0.8698	0.0545	-0.8698	0.0545	0.0000	0.0000
381	481	-0.8698	0.0545	-0.8698	0.0545	0.0000	0.0000
481	581	-0.8698	0.0545	-0.8698	0.0545	0.0000	0.0000
2	202	-0.4000	-0.4984	-0.4000	-0.4984	0.0000	0.0000
202	302	-0.4000	-0.4984	-0.4000	-0.4984	0.0000	0.0000
302	402	-0.4000	-0.4984	-0.4000	-0.4984	0.0000	0.0000
402	502	-0.4000	-0.4984	-0.4000	-0.4984	0.0000	0.0000
5	205	0.0000	-0.3697	0.0000	-0.3697	0.0000	0.0000
205	305	0.0000	-0.3697	0.0000	-0.3697	0.0000	0.0000
305	405	0.0000	-0.3697	0.0000	-0.3697	0.0000	0.0000
405	505	0.0000	-0.3697	0.0000	-0.3697	0.0000	0.0000
8	208	0.0000	-0.3780	0.0000	-0.3780	0.0000	0.0000
208	308	0.0000	-0.3780	0.0000	-0.3780	0.0000	0.0000
308	408	0.0000	-0.3780	0.0000	-0.3780	0.0000	0.0000

Table B.12
Power flow branch solution in IEEE 30-bus system (Part 3)

From	To	Psend (p.u.)	Qsend (p.u.)	Prec (p.u.)	Qrec (p.u.)	Ploss (p.u.)	Qloss (p.u.)
408	508	0.0000	-0.3780	0.0000	-0.3780	0.0000	0.0000
11	211	0.0000	-0.1671	0.0000	-0.1671	0.0000	0.0000
211	311	0.0000	-0.1671	0.0000	-0.1671	0.0000	0.0000
311	411	0.0000	-0.1671	0.0000	-0.1671	0.0000	0.0000
411	511	0.0000	-0.1671	0.0000	-0.1671	0.0000	0.0000
13	213	0.0000	-0.1109	0.0000	-0.1109	0.0000	0.0000
213	313	0.0000	-0.1109	0.0000	-0.1109	0.0000	0.0000
313	413	0.0000	-0.1109	0.0000	-0.1109	0.0000	0.0000
413	513	0.0000	-0.1109	0.0000	-0.1109	0.0000	0.0000

The total P loss and Q loss are 0.1754 (p.u.) and 0.3308 (p.u.), individually.

Table B.13
System (branch) setting data (Part 1)

From	To	Resistance	Reactance	Capacitance (Y/2)	Tap	Remark
1	2	0.01920	0.05750	0.02640	0.00000	
1	3	0.04520	0.16520	0.02040	0.00000	
2	4	0.05700	0.17370	0.01840	0.00000	
3	4	0.01320	0.03790	0.00420	0.00000	
2	5	0.04720	0.19830	0.02090	0.00000	
2	6	0.05810	0.17630	0.01870	0.00000	
4	6	0.01190	0.04140	0.00450	0.00000	
5	7	0.04600	0.11600	0.01020	0.00000	
6	7	0.02670	0.08200	0.00850	0.00000	
6	8	0.01200	0.04200	0.00450	0.00000	
9	11	0.00000	0.20800	0.00000	0.00000	
9	10	0.00000	0.11000	0.00000	0.00000	
12	13	0.00000	0.14000	0.00000	0.00000	
12	14	0.12310	0.25590	0.00000	0.00000	
12	15	0.06620	0.13040	0.00000	0.00000	
12	16	0.09450	0.19870	0.00000	0.00000	
14	15	0.22100	0.19970	0.00000	0.00000	
16	17	0.05240	0.19230	0.00000	0.00000	
15	18	0.10730	0.21850	0.00000	0.00000	
18	19	0.06390	0.12920	0.00000	0.00000	
19	20	0.03400	0.06800	0.00000	0.00000	
10	20	0.09360	0.20900	0.00000	0.00000	
10	17	0.03240	0.08450	0.00000	0.00000	
10	21	0.03480	0.07490	0.00000	0.00000	
10	22	0.07270	0.14990	0.00000	0.00000	
21	22	0.01160	0.02360	0.00000	0.00000	
15	23	0.10000	0.20200	0.00000	0.00000	
22	24	0.11500	0.17900	0.00000	0.00000	
23	24	0.13200	0.27000	0.00000	0.00000	
24	25	0.18850	0.32920	0.00000	0.00000	
25	26	0.25440	0.38000	0.00000	0.00000	
25	27	0.10930	0.20870	0.00000	0.00000	
27	29	0.21980	0.41530	0.00000	0.00000	
27	30	0.32020	0.60270	0.00000	0.00000	
29	30	0.23990	0.45330	0.00000	0.00000	
8	28	0.06360	0.20000	0.02140	0.00000	

Table B.14
System (branch) setting data (Part 2)

From	To	Resistance	Reactance	Capacitance (Y/2)	Tap	Remark
6	28	0.01690	0.05990	0.00650	0.00000	
36	39	0.00000	0.20800	0.00000	1.02250	
56	40	0.00000	0.55600	0.00000	1.03200	
44	52	0.00000	0.25600	0.00000	1.07300	
48	47	0.00000	0.39600	0.00000	1.03306	
6	36	0.00000	0.00000	0.00000	0.00000	CB1
39	9	0.00000	0.00000	0.00000	0.00000	CB1
6	56	0.00000	0.00000	0.00000	0.00000	CB1
40	10	0.00000	0.00000	0.00000	0.00000	CB1
4	44	0.00000	0.00000	0.00000	0.00000	CB1
52	12	0.00000	0.00000	0.00000	0.00000	CB1
28	48	0.00000	0.00000	0.00000	0.00000	CB1
47	27	0.00000	0.00000	0.00000	0.00000	CB1
1	201	0.00000	0.00000	0.00000	0.00000	CB1
201	301	0.00000	0.00000	0.00000	0.00000	CB1
301	401	0.00000	0.00000	0.00000	0.00000	CB1
401	501	0.00000	0.00000	0.00000	0.00000	CB1
1	271	0.00000	0.00000	0.00000	0.00000	CB1
271	371	0.00000	0.00000	0.00000	0.00000	CB1
371	471	0.00000	0.00000	0.00000	0.00000	CB1
471	571	0.00000	0.00000	0.00000	0.00000	CB1
1	281	0.00000	0.00000	0.00000	0.00000	CB1
281	381	0.00000	0.00000	0.00000	0.00000	CB1
381	481	0.00000	0.00000	0.00000	0.00000	CB1
481	581	0.00000	0.00000	0.00000	0.00000	CB1
2	202	0.00000	0.00000	0.00000	0.00000	CB1
202	302	0.00000	0.00000	0.00000	0.00000	CB1
302	402	0.00000	0.00000	0.00000	0.00000	CB1
402	502	0.00000	0.00000	0.00000	0.00000	CB1
5	205	0.00000	0.00000	0.00000	0.00000	CB1
205	305	0.00000	0.00000	0.00000	0.00000	CB1
305	405	0.00000	0.00000	0.00000	0.00000	CB1
405	505	0.00000	0.00000	0.00000	0.00000	CB1
8	208	0.00000	0.00000	0.00000	0.00000	CB1
208	308	0.00000	0.00000	0.00000	0.00000	CB1
308	408	0.00000	0.00000	0.00000	0.00000	CB1
408	508	0.00000	0.00000	0.00000	0.00000	CB1

Table B.15
System (branch) setting data (Part 3)

From	To	Resistance	Reactance	Capacitance (Y/2)	Tap	Remark
11	211	0.00000	0.00000	0.00000	0.00000	CB1
211	311	0.00000	0.00000	0.00000	0.00000	CB1
311	411	0.00000	0.00000	0.00000	0.00000	CB1
411	511	0.00000	0.00000	0.00000	0.00000	CB1
13	213	0.00000	0.00000	0.00000	0.00000	CB1
213	313	0.00000	0.00000	0.00000	0.00000	CB1
313	413	0.00000	0.00000	0.00000	0.00000	CB1
413	513	0.00000	0.00000	0.00000	0.00000	CB1

Table B.16
Power flow condition setting data (Part 1)

Node	To	PG	QG	PL	QL	QC	Name
1	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Glen LynA1
2	0.0000	0.0000	0.0000	0.2170	0.1270	0.0000	Claytor1
3	0.0000	0.0000	0.0000	0.0240	0.0120	0.0000	Kumis
4	0.0000	0.0000	0.0000	0.0760	0.0160	0.0000	Hancock
5	0.0000	0.0000	0.0000	0.9420	0.1900	0.0000	Fieldale1
6	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Roanoke
7	0.0000	0.0000	0.0000	0.2280	0.1090	0.0000	Blaine
8	0.0000	0.0000	0.0000	0.3000	0.3000	0.0000	Reusens1
9	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	1kVRoanoke
10	0.0000	0.0000	0.0000	0.0580	0.0200	0.1740	33kVRoanoke
11	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	11kVRoanoke1
12	0.0000	0.0000	0.0000	0.1120	0.0750	0.0000	33kVHancock
13	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	11kVHancock1
14	0.0000	0.0000	0.0000	0.0620	0.0160	0.0000	33kVBus_14
15	0.0000	0.0000	0.0000	0.0820	0.0250	0.0000	33kVBus_15
16	0.0000	0.0000	0.0000	0.0350	0.0180	0.0000	33kVBus_16
17	0.0000	0.0000	0.0000	0.0900	0.0580	0.0000	33kVBus_17
18	0.0000	0.0000	0.0000	0.0320	0.0090	0.0000	33kVBus_18
19	0.0000	0.0000	0.0000	0.0950	0.0340	0.0000	33kVBus_19
20	0.0000	0.0000	0.0000	0.0220	0.0070	0.0000	33kVBus_20
21	0.0000	0.0000	0.0000	0.1750	0.1120	0.0000	33kVBus_21
22	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	33kVBus_22
23	0.0000	0.0000	0.0000	0.0320	0.0160	0.0000	33kVBus_23
24	0.0000	0.0000	0.0000	0.0870	0.0670	0.0413	33kVBus_24
25	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	33kVBus_25
26	0.0000	0.0000	0.0000	0.0350	0.0230	0.0000	33kVBus_26
27	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	33kCloverdle
28	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Cloverdle
29	0.0000	0.0000	0.0000	0.0240	0.0090	0.0000	33kVBus_29
30	0.0000	0.0000	0.0000	0.1060	0.0190	0.0000	33kVBus_30
36	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Glen LynA2
39	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Claytor2
40	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Fieldale2
44	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Reusens2
47	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	11kVRoanoke2
48	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	11kVHancock2
52	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Glen LynB2

Table B.17
Power flow condition setting data (Part 2)

Node	To	PG	QG	PL	QL	QC	Name
56	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Glen LynC2
201	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
202	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
205	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
208	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
211	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
213	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
271	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
281	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
301	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
302	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
305	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
308	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
311	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
313	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
371	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
381	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
401	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
402	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
405	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
408	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
411	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
413	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
471	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
481	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
501	1.0600	0.0000	0.0000	0.0000	0.0000	0.0000	
502	1.0430	0.4000	0.0000	0.0000	0.0000	0.0000	
505	1.0100	0.0000	0.3700	0.0000	0.0000	0.0000	
508	1.0100	0.0000	0.3730	0.0000	0.0000	0.0000	
511	1.0820	0.0000	0.1620	0.0000	0.0000	0.0000	
513	1.0710	0.0000	0.1060	0.0000	0.0000	0.0000	
571	1.0600	0.8698	0.0000	0.0000	0.0000	0.0000	
581	1.0600	0.8698	0.0000	0.0000	0.0000	0.0000	

Table B.18
Generator constants with implemented generator controller

Node	AVR	OEL	PSS	GOV	GMVA	GMW	GPF	MG	DG	PLM	Name
501	X	X		X	100.0	87.5	0.875	6.0	0.0	5.0	G1A
571	X	X		X	100.0	87.5	0.875	6.0	0.0	5.0	G1B
581	X	X		X	100.0	87.5	0.875	6.0	0.0	5.0	G1C
502	X	X		X	70.0	61.3	0.875	6.0	0.0	5.0	G2
505	X				50.0	0.0	0.000	1.5	0.0	0.0	C05
508	X				50.0	0.0	0.000	1.5	0.0	0.0	C08
511	X				25.0	0.0	0.000	1.5	0.0	0.0	C11
513	X				25.0	0.0	0.000	1.5	0.0	0.0	C13

Table B.19
Generator constants of the used generator model

Node	RA	XL	XD	XDD	XDDD	XFLD	XKLD	XQ	XQDD	XKLQ	TDD	TDDD	RFD	RKD	TQDD	RKQ
501	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
571	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
581	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
502	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
505	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
508	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
511	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
513	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195

Table B.20
Initial condition of synchronous generator and condenser

Node	AGG	VT	PG	QG	TQG	EF	CF	CDD	CQQ	FGD	FGQ
501	55.08	1.060	0.8699	-0.0546	0.8710	1.7014	1.7014	0.6434	0.5119	0.7523	-0.7551
571	55.08	1.060	0.8698	-0.0545	0.8709	1.7013	1.7013	0.6433	0.5119	0.7524	-0.7550
581	55.08	1.060	0.8698	-0.0545	0.8709	1.7013	1.7013	0.6433	0.5119	0.7524	-0.7550
502	17.53	1.043	0.5714	0.7120	0.5727	2.3926	2.3926	0.8419	0.2394	1.1508	-0.3531
505	-14.18	1.010	0.0000	0.7394	0.0009	2.2546	2.2546	0.7321	0.0004	1.1747	-0.0006
508	-11.84	1.010	0.0000	0.7560	0.0009	2.2825	2.2825	0.7485	0.0004	1.1784	-0.0006
511	-14.12	1.082	0.0000	0.6684	0.0006	2.1321	2.1321	0.6177	0.0003	1.2210	-0.0004
513	-14.97	1.071	0.0000	0.4437	0.0003	1.7752	1.7752	0.4143	0.0002	1.1642	-0.0002

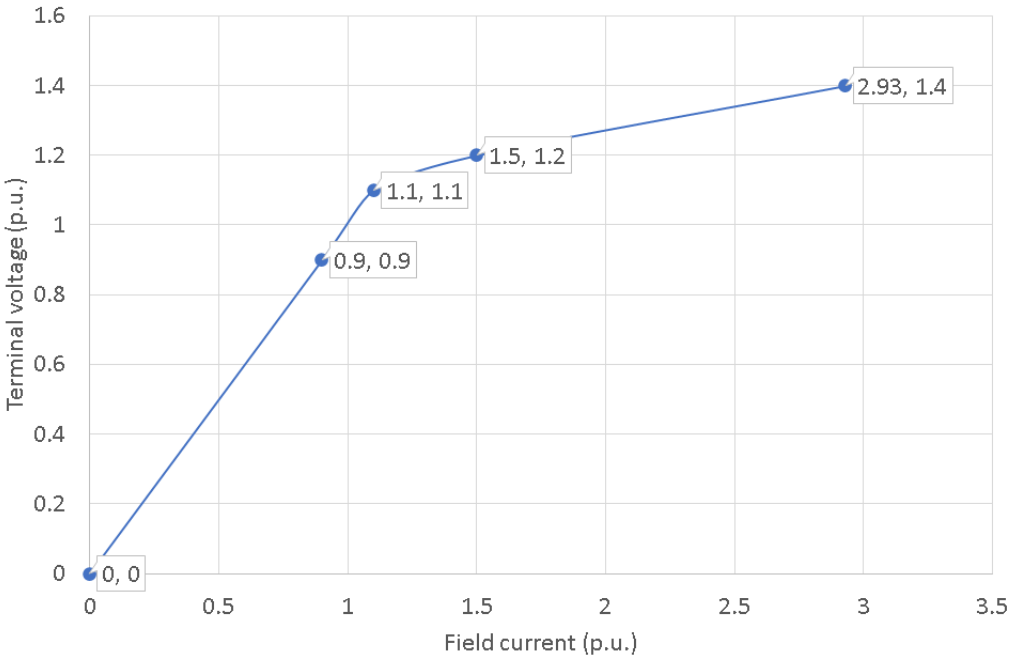


Figure B.3: Generator's saturation characteristics

B.3 IEEE 57-bus System

The system diagram is shown in Fig. B.4. Power flow solutions are summarized in Tables B.21, B.22, B.22, B.24, B.25, B.26, B.27, B.28, and B.29. The system MVA is 100 MVA. The power flow setting data are also provided in Tables B.30, B.31, B.32, B.33, B.34, B.35, B.36 and B.37. It is noted that circuit breakers with no impedance are inserted between the main grid and individual power equipment.

Initial conditions of the dynamic simulation with generator constants are sorted out in Tables B.39, B.40 and B.41.

It is noted that the generator's saturation characteristics is used for the IEEE 57-bus systems (Fig. B.3).

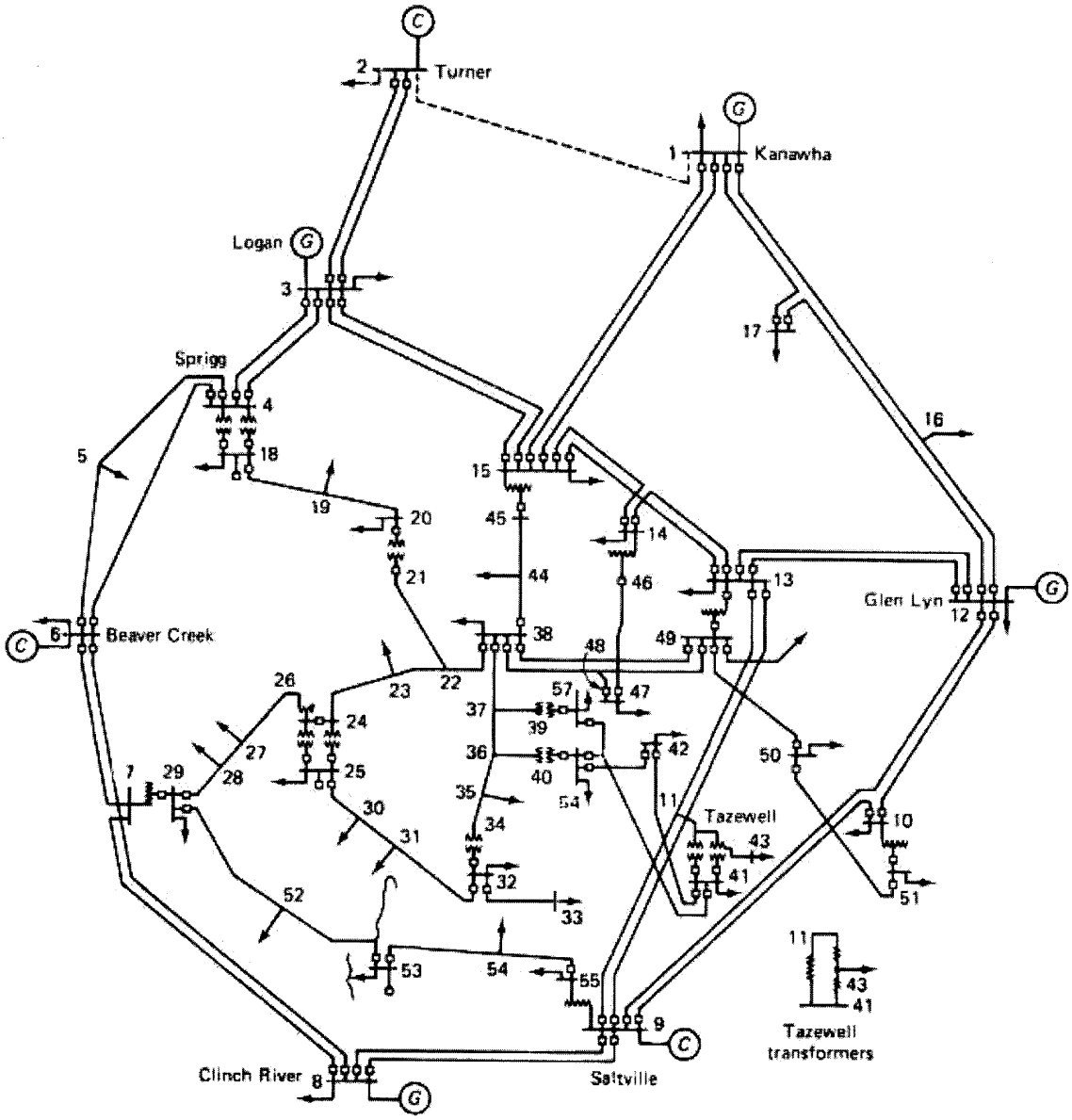


Figure B.4: Diagram of IEEE 57-bus system

Table B.21
Power flow node solution in IEEE 57-bus system (part 1)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
1	1.0400	0.00	0.0000	0.0000	0.5500	0.1700	0.0000	Kanawha1
2	1.0100	-1.19	0.0000	0.0000	0.0300	0.8800	0.0000	Turner1
3	0.9850	-5.98	0.0000	0.0000	0.4100	0.2100	0.0000	Logan1
4	0.9808	-7.33	0.0000	0.0000	0.0000	0.0000	0.0000	Sprigg
5	0.9765	-8.53	0.0000	0.0000	0.1300	0.0400	0.0000	Bus5
6	0.9800	-8.66	0.0000	0.0000	0.7500	0.0200	0.0000	BeaverCk1
7	0.9843	-7.59	0.0000	0.0000	0.0000	0.0000	0.0000	Bus7
8	1.0050	-4.47	0.0000	0.0000	1.5000	0.2200	0.0000	ClinchRv1
9	0.9800	-9.57	0.0000	0.0000	1.2100	0.2600	0.0000	Saltville1
10	0.9863	-11.44	0.0000	0.0000	0.0500	0.0200	0.0000	Bus10
11	0.9740	-10.18	0.0000	0.0000	0.0000	0.0000	0.0000	Tazewell
12	1.0150	-10.46	0.0000	0.0000	3.7700	0.2400	0.0000	Glen Lyn1
13	0.9789	-9.79	0.0000	0.0000	0.1800	0.0230	0.0000	Bus13
14	0.9703	-9.34	0.0000	0.0000	0.1050	0.0530	0.0000	Bus14
15	0.9881	-7.18	0.0000	0.0000	0.2200	0.0500	0.0000	Bus15
16	1.0134	-8.84	0.0000	0.0000	0.4300	0.0300	0.0000	Bus16
17	1.0175	-5.39	0.0000	0.0000	0.4200	0.0800	0.0000	Bus17
18	1.0006	-11.72	0.0000	0.0000	0.2720	0.0980	0.0999	Sprigg
19	0.9702	-13.22	0.0000	0.0000	0.0330	0.0060	0.0000	Bus19
20	0.9639	-13.44	0.0000	0.0000	0.0230	0.0100	0.0000	Bus20
21	1.0087	-12.92	0.0000	0.0000	0.0000	0.0000	0.0000	Bus21
22	1.0100	-12.86	0.0000	0.0000	0.0000	0.0000	0.0000	Bus22
23	1.0086	-12.93	0.0000	0.0000	0.0630	0.0210	0.0000	Bus23
24	0.9998	-13.29	0.0000	0.0000	0.0000	0.0000	0.0000	Bus24
25	0.9843	-18.17	0.0000	0.0000	0.0630	0.0320	0.0593	Bus25
26	0.9594	-12.98	0.0000	0.0000	0.0000	0.0000	0.0000	Bus26
27	0.9819	-11.51	0.0000	0.0000	0.0930	0.0050	0.0000	Bus27
28	0.9970	-10.47	0.0000	0.0000	0.0460	0.0230	0.0000	Bus28
29	1.0105	-9.76	0.0000	0.0000	0.1700	0.0260	0.0000	Bus29
30	0.9643	-18.71	0.0000	0.0000	0.0360	0.0180	0.0000	Bus30
31	0.9373	-19.37	0.0000	0.0000	0.0580	0.0290	0.0000	Bus31
32	0.9508	-18.49	0.0000	0.0000	0.0160	0.0080	0.0000	Bus32
33	0.9485	-18.53	0.0000	0.0000	0.0380	0.0190	0.0000	Bus33
34	0.9596	-14.14	0.0000	0.0000	0.0000	0.0000	0.0000	Bus34
35	0.9665	-13.90	0.0000	0.0000	0.0600	0.0300	0.0000	Bus35

Table B.22
Power flow node solution in IEEE 57-bus system (part 2)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
36	0.9761	-13.62	0.0000	0.0000	0.0000	0.0000	0.0000	Bus36
37	0.9852	-13.44	0.0000	0.0000	0.0000	0.0000	0.0000	Bus37
38	1.0130	-12.72	0.0000	0.0000	0.1400	0.0700	0.0000	Bus38
39	0.9831	-13.48	0.0000	0.0000	0.0000	0.0000	0.0000	Bus39
40	0.9731	-13.65	0.0000	0.0000	0.0000	0.0000	0.0000	Bus40
41	0.9963	-14.06	0.0000	0.0000	0.0630	0.0300	0.0000	Tazewell
42	0.9667	-15.52	0.0000	0.0000	0.0710	0.0440	0.0000	Bus42
43	1.0096	-11.34	0.0000	0.0000	0.0200	0.0100	0.0000	Tazewell
44	1.0170	-11.85	0.0000	0.0000	0.1200	0.0180	0.0000	Bus44
45	1.0361	-9.26	0.0000	0.0000	0.0000	0.0000	0.0000	Bus45
46	1.0599	-11.10	0.0000	0.0000	0.0000	0.0000	0.0000	Bus46
47	1.0334	-12.50	0.0000	0.0000	0.2970	0.1160	0.0000	Bus47
48	1.0275	-12.60	0.0000	0.0000	0.0000	0.0000	0.0000	Bus48
49	1.0364	-12.92	0.0000	0.0000	0.1800	0.0850	0.0000	Bus49
50	1.0234	-13.40	0.0000	0.0000	0.2100	0.1050	0.0000	Bus50
51	1.0523	-12.52	0.0000	0.0000	0.1800	0.0530	0.0000	Bus51
52	0.9811	-11.51	0.0000	0.0000	0.0490	0.0220	0.0000	Bus52
53	0.9719	-12.27	0.0000	0.0000	0.2000	0.1000	0.0631	Bus53
54	0.9969	-11.71	0.0000	0.0000	0.0410	0.0140	0.0000	Bus54
55	1.0310	-10.79	0.0000	0.0000	0.0680	0.0340	0.0000	Saltville
56	0.9685	-16.05	0.0000	0.0000	0.0760	0.0220	0.0000	Bus56
57	0.9650	-16.57	0.0000	0.0000	0.0670	0.0200	0.0000	Bus57
201	1.0400	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	Kanawha2A
202	1.0100	-1.19	0.0000	0.0000	0.0000	0.0000	0.0000	Turner2
203	0.9850	-5.98	0.0000	0.0000	0.0000	0.0000	0.0000	Logan2
206	0.9800	-8.66	0.0000	0.0000	0.0000	0.0000	0.0000	BeaverCk2
208	1.0050	-4.47	0.0000	0.0000	0.0000	0.0000	0.0000	ClinchRv2A
209	0.9800	-9.57	0.0000	0.0000	0.0000	0.0000	0.0000	Saltville2
212	1.0150	-10.46	0.0000	0.0000	0.0000	0.0000	0.0000	Glen Lyn2A
271	1.0400	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	Kanawha2B
272	1.0150	-10.46	0.0000	0.0000	0.0000	0.0000	0.0000	Glen Lyn2B
278	1.0050	-4.47	0.0000	0.0000	0.0000	0.0000	0.0000	ClinchRv2B
281	1.0400	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	Kanawha2C
288	1.0050	-4.47	0.0000	0.0000	0.0000	0.0000	0.0000	ClinchRv2C
301	1.0400	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.23
Power flow node solution in IEEE 57-bus system (part 3)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
302	1.0100	-1.19	0.0000	0.0000	0.0000	0.0000	0.0000	
303	0.9850	-5.98	0.0000	0.0000	0.0000	0.0000	0.0000	
306	0.9800	-8.66	0.0000	0.0000	0.0000	0.0000	0.0000	
308	1.0050	-4.47	0.0000	0.0000	0.0000	0.0000	0.0000	
309	0.9800	-9.57	0.0000	0.0000	0.0000	0.0000	0.0000	
312	1.0150	-10.46	0.0000	0.0000	0.0000	0.0000	0.0000	
371	1.0400	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
372	1.0150	-10.46	0.0000	0.0000	0.0000	0.0000	0.0000	
378	1.0050	-4.47	0.0000	0.0000	0.0000	0.0000	0.0000	
381	1.0400	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
388	1.0050	-4.47	0.0000	0.0000	0.0000	0.0000	0.0000	
401	1.0400	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
402	1.0100	-1.19	0.0000	0.0000	0.0000	0.0000	0.0000	
403	0.9850	-5.98	0.0000	0.0000	0.0000	0.0000	0.0000	
406	0.9800	-8.66	0.0000	0.0000	0.0000	0.0000	0.0000	
408	1.0050	-4.47	0.0000	0.0000	0.0000	0.0000	0.0000	
409	0.9800	-9.57	0.0000	0.0000	0.0000	0.0000	0.0000	
412	1.0150	-10.46	0.0000	0.0000	0.0000	0.0000	0.0000	
471	1.0400	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
472	1.0150	-10.46	0.0000	0.0000	0.0000	0.0000	0.0000	
478	1.0050	-4.47	0.0000	0.0000	0.0000	0.0000	0.0000	
481	1.0400	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
488	1.0050	-4.47	0.0000	0.0000	0.0000	0.0000	0.0000	
501	1.0400	0.00	1.5954	0.4300	0.0000	0.0000	0.0000	
502	1.0100	-1.19	0.0000	-0.0077	0.0000	0.0000	0.0000	
503	0.9850	-5.98	0.4000	-0.0110	0.0000	0.0000	0.0000	
506	0.9800	-8.66	0.0000	0.0071	0.0000	0.0000	0.0000	
508	1.0050	-4.47	1.5000	0.2066	0.0000	0.0000	0.0000	
509	0.9800	-9.57	0.0000	0.0193	0.0000	0.0000	0.0000	
512	1.0150	-10.46	1.5500	0.6425	0.0000	0.0000	0.0000	
571	1.0400	0.00	1.5954	0.4301	0.0000	0.0000	0.0000	
572	1.0150	-10.46	1.5500	0.6425	0.0000	0.0000	0.0000	
578	1.0050	-4.47	1.5000	0.2066	0.0000	0.0000	0.0000	
581	1.0400	0.00	1.5954	0.4300	0.0000	0.0000	0.0000	
588	1.0050	-4.47	1.5000	0.2067	0.0000	0.0000	0.0000	

Table B.24
Power flow node solution in IEEE 57-bus system (part 4)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
604	0.9808	-7.33	0.0000	0.0000	0.0000	0.0000	0.0000	
607	0.9843	-7.59	0.0000	0.0000	0.0000	0.0000	0.0000	
609	0.9800	-9.57	0.0000	0.0000	0.0000	0.0000	0.0000	
610	0.9863	-11.44	0.0000	0.0000	0.0000	0.0000	0.0000	
611	0.9740	-10.18	0.0000	0.0000	0.0000	0.0000	0.0000	
613	0.9789	-9.79	0.0000	0.0000	0.0000	0.0000	0.0000	
614	0.9703	-9.34	0.0000	0.0000	0.0000	0.0000	0.0000	
615	0.9881	-7.18	0.0000	0.0000	0.0000	0.0000	0.0000	
618	1.0006	-11.72	0.0000	0.0000	0.0000	0.0000	0.0000	
620	0.9639	-13.44	0.0000	0.0000	0.0000	0.0000	0.0000	
621	1.0087	-12.92	0.0000	0.0000	0.0000	0.0000	0.0000	
624	0.9998	-13.29	0.0000	0.0000	0.0000	0.0000	0.0000	
625	0.9843	-18.17	0.0000	0.0000	0.0000	0.0000	0.0000	
626	0.9594	-12.98	0.0000	0.0000	0.0000	0.0000	0.0000	
629	1.0105	-9.76	0.0000	0.0000	0.0000	0.0000	0.0000	
632	0.9508	-18.49	0.0000	0.0000	0.0000	0.0000	0.0000	
634	0.9596	-14.14	0.0000	0.0000	0.0000	0.0000	0.0000	
639	0.9831	-13.48	0.0000	0.0000	0.0000	0.0000	0.0000	
640	0.9731	-13.65	0.0000	0.0000	0.0000	0.0000	0.0000	
641	0.9963	-14.06	0.0000	0.0000	0.0000	0.0000	0.0000	
643	1.0096	-11.34	0.0000	0.0000	0.0000	0.0000	0.0000	
645	1.0361	-9.26	0.0000	0.0000	0.0000	0.0000	0.0000	
646	1.0599	-11.10	0.0000	0.0000	0.0000	0.0000	0.0000	
649	1.0364	-12.92	0.0000	0.0000	0.0000	0.0000	0.0000	
651	1.0523	-12.52	0.0000	0.0000	0.0000	0.0000	0.0000	
655	1.0310	-10.79	0.0000	0.0000	0.0000	0.0000	0.0000	
656	0.9685	-16.05	0.0000	0.0000	0.0000	0.0000	0.0000	
657	0.9650	-16.57	0.0000	0.0000	0.0000	0.0000	0.0000	
704	0.9808	-7.33	0.0000	0.0000	0.0000	0.0000	0.0000	
711	0.9740	-10.18	0.0000	0.0000	0.0000	0.0000	0.0000	
718	1.0006	-11.72	0.0000	0.0000	0.0000	0.0000	0.0000	
724	0.9998	-13.29	0.0000	0.0000	0.0000	0.0000	0.0000	
725	0.9843	-18.17	0.0000	0.0000	0.0000	0.0000	0.0000	
824	0.9998	-13.29	0.0000	0.0000	0.0000	0.0000	0.0000	
Total			12.7861	3.2027	12.5080	3.3640	0.2223	

Table B.25
Power flow branch solution in IEEE 57-bus system (Part 1)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
1	2	1.0204	0.7509	1.0073	0.8421	0.0132	-0.0912
2	3	0.9773	-0.0456	0.9494	-0.0437	0.0279	-0.0020
3	4	0.6020	-0.0816	0.5978	-0.0588	0.0042	-0.0229
4	5	0.1379	-0.0443	0.1366	-0.0223	0.0013	-0.0220
4	6	0.1415	-0.0509	0.1406	-0.0207	0.0010	-0.0302
6	7	-0.1776	-0.0184	-0.1782	0.0049	0.0007	-0.0233
6	8	-0.4253	-0.0659	-0.4317	-0.0525	0.0064	-0.0135
8	9	1.7801	0.1986	1.7485	0.0917	0.0315	0.1069
9	10	0.1717	-0.0925	0.1703	-0.0559	0.0013	-0.0365
9	11	0.1289	0.0203	0.1285	0.0395	0.0005	-0.0193
9	12	0.0256	-0.1590	0.0245	-0.0868	0.0011	-0.0722
9	13	0.0231	-0.0199	0.0231	0.0190	0.0000	-0.0389
13	14	-0.1035	0.2229	-0.1044	0.2305	0.0009	-0.0076
13	15	-0.4889	0.0487	-0.4957	0.0489	0.0068	-0.0003
1	15	1.4899	0.3382	1.4509	0.2406	0.0390	0.0976
1	16	0.7927	-0.0085	0.7664	-0.0704	0.0263	0.0619
1	17	0.9332	0.0395	0.9140	-0.0175	0.0192	0.0569
3	15	0.3374	-0.1830	0.3351	-0.1376	0.0023	-0.0454
5	6	0.0066	-0.0623	0.0065	-0.0507	0.0001	-0.0117
7	8	-0.7793	-0.1225	-0.7882	-0.1489	0.0089	0.0264
10	12	-0.1760	-0.2008	-0.1779	-0.1764	0.0019	-0.0244
11	13	-0.0993	-0.0441	-0.0996	-0.0270	0.0003	-0.0171
12	13	-0.0047	0.6028	-0.0116	0.6403	0.0069	-0.0375
12	16	-0.3343	0.0878	-0.3364	0.1004	0.0021	-0.0126
12	17	-0.4844	0.0913	-0.4940	0.0975	0.0095	-0.0061
14	15	-0.6882	-0.0959	-0.6970	-0.1097	0.0087	0.0138
18	19	0.0463	0.0137	0.0452	0.0121	0.0011	0.0016
19	20	0.0122	0.0061	0.0122	0.0061	0.0001	0.0001
21	22	-0.0108	-0.0041	-0.0108	-0.0041	0.0000	0.0000
22	23	0.0965	0.0298	0.0964	0.0297	0.0001	0.0002
23	24	0.0334	0.0087	0.0332	0.0168	0.0002	-0.0081
26	27	-0.1055	-0.0155	-0.1076	-0.0186	0.0020	0.0031
27	28	-0.2006	-0.0236	-0.2032	-0.0277	0.0026	0.0040
28	29	-0.2492	-0.0507	-0.2519	-0.0545	0.0027	0.0038
25	30	0.0757	0.0468	0.0746	0.0451	0.0011	0.0017

Table B.26
Power flow branch solution in IEEE 57-bus system (Part 2)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
30	31	0.0386	0.0271	0.0379	0.0259	0.0008	0.0012
31	32	-0.0201	-0.0031	-0.0204	-0.0034	0.0002	0.0004
32	33	0.0381	0.0191	0.0380	0.0190	0.0001	0.0001
34	35	-0.0745	-0.0373	-0.0748	-0.0349	0.0004	-0.0024
35	36	-0.1348	-0.0649	-0.1359	-0.0647	0.0010	-0.0002
36	37	-0.1705	-0.1057	-0.1718	-0.1072	0.0012	0.0015
37	38	-0.2103	-0.1366	-0.2146	-0.1411	0.0042	0.0045
37	39	0.0386	0.0294	0.0385	0.0293	0.0001	0.0001
36	40	0.0347	0.0410	0.0346	0.0409	0.0001	0.0001
22	38	-0.1073	-0.0339	-0.1076	-0.0343	0.0002	0.0004
41	42	0.0888	0.0326	0.0869	0.0295	0.0019	0.0032
41	43	-0.1159	-0.0294	-0.1159	-0.0354	0.0000	0.0059
38	44	-0.2434	0.0528	-0.2452	0.0513	0.0017	0.0015
46	47	0.4789	0.2542	0.4728	0.2398	0.0060	0.0143
47	48	0.1758	0.1238	0.1751	0.1228	0.0008	0.0010
48	49	0.0008	-0.0735	0.0004	-0.0690	0.0004	-0.0045
49	50	0.0967	0.0446	0.0958	0.0432	0.0008	0.0014
50	51	-0.1142	-0.0618	-0.1164	-0.0653	0.0022	0.0035
29	52	0.1792	0.0233	0.1746	0.0173	0.0046	0.0060
52	53	0.1256	-0.0047	0.1243	-0.0063	0.0012	0.0016
53	54	-0.0757	-0.0432	-0.0772	-0.0450	0.0015	0.0019
54	55	-0.1182	-0.0590	-0.1212	-0.0630	0.0030	0.0040
44	45	-0.3652	0.0333	-0.3733	0.0214	0.0081	0.0119
56	41	-0.0543	0.0067	-0.0560	0.0050	0.0018	0.0018
56	42	-0.0158	0.0147	-0.0159	0.0145	0.0001	0.0002
57	56	-0.0285	0.0061	-0.0286	0.0059	0.0002	0.0002
38	49	-0.0466	-0.1050	-0.0480	-0.1040	0.0014	-0.0009
38	48	-0.1722	-0.1932	-0.1742	-0.1964	0.0020	0.0031
604	618	0.1396	0.0244	0.1396	0.0135	0.0000	0.0109
704	718	0.1787	0.0120	0.1787	-0.0017	0.0000	0.0137
621	620	0.0108	0.0041	0.0108	0.0039	0.0000	0.0001
624	625	0.0708	0.0162	0.0708	0.0100	0.0000	0.0062
724	725	0.0680	0.0155	0.0680	0.0096	0.0000	0.0060
824	626	-0.1055	-0.0149	-0.1055	-0.0155	0.0000	0.0006
607	629	0.6011	0.1274	0.6011	0.1038	0.0000	0.0236

Table B.27
Power flow branch solution in IEEE 57-bus system (Part 3)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
634	632	0.0745	0.0373	0.0745	0.0305	0.0000	0.0068
611	641	0.0919	0.0352	0.0919	0.0282	0.0000	0.0070
615	645	0.3733	-0.0078	0.3733	-0.0214	0.0000	0.0136
614	646	0.4789	0.2734	0.4789	0.2542	0.0000	0.0192
610	651	0.2964	0.1249	0.2964	0.1183	0.0000	0.0065
613	649	0.3242	0.3376	0.3242	0.3026	0.0000	0.0350
711	643	0.1359	0.0484	0.1359	0.0454	0.0000	0.0031
640	656	0.0346	0.0409	0.0346	0.0375	0.0000	0.0033
639	657	0.0385	0.0293	0.0385	0.0261	0.0000	0.0032
609	655	0.1892	0.1022	0.1892	0.0970	0.0000	0.0051
4	604	0.1396	0.0244	0.1396	0.0244	0.0000	0.0000
618	18	0.1396	0.0135	0.1396	0.0135	0.0000	0.0000
4	704	0.1787	0.0120	0.1787	0.0120	0.0000	0.0000
718	18	0.1787	-0.0017	0.1787	-0.0017	0.0000	0.0000
21	621	0.0108	0.0041	0.0108	0.0041	0.0000	0.0000
620	20	0.0108	0.0040	0.0108	0.0040	0.0000	0.0000
24	624	0.0708	0.0162	0.0708	0.0162	0.0000	0.0000
625	25	0.0708	0.0100	0.0708	0.0100	0.0000	0.0000
24	724	0.0680	0.0155	0.0680	0.0155	0.0000	0.0000
725	25	0.0680	0.0096	0.0680	0.0096	0.0000	0.0000
24	824	-0.1055	-0.0149	-0.1055	-0.0149	0.0000	0.0000
626	26	-0.1055	-0.0155	-0.1055	-0.0155	0.0000	0.0000
7	607	0.6011	0.1274	0.6011	0.1274	0.0000	0.0000
629	29	0.6011	0.1038	0.6011	0.1038	0.0000	0.0000
34	634	0.0745	0.0373	0.0745	0.0373	0.0000	0.0000
632	32	0.0745	0.0305	0.0745	0.0305	0.0000	0.0000
11	611	0.0919	0.0352	0.0919	0.0352	0.0000	0.0000
641	41	0.0919	0.0282	0.0919	0.0282	0.0000	0.0000
15	615	0.3733	-0.0078	0.3733	-0.0078	0.0000	0.0000
645	45	0.3733	-0.0214	0.3733	-0.0214	0.0000	0.0000
14	614	0.4789	0.2734	0.4789	0.2734	0.0000	0.0000
646	46	0.4789	0.2542	0.4789	0.2542	0.0000	0.0000
10	610	0.2964	0.1249	0.2964	0.1249	0.0000	0.0000
651	51	0.2964	0.1183	0.2964	0.1183	0.0000	0.0000
13	613	0.3242	0.3376	0.3242	0.3376	0.0000	0.0000
649	49	0.3242	0.3026	0.3242	0.3026	0.0000	0.0000

Table B.28
Power flow branch solution in IEEE 57-bus system (Part 4)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
11	711	0.1359	0.0484	0.1359	0.0484	0.0000	0.0000
643	43	0.1359	0.0453	0.1359	0.0453	0.0000	0.0000
40	640	0.0346	0.0409	0.0346	0.0409	0.0000	0.0000
656	56	0.0346	0.0376	0.0346	0.0376	0.0000	0.0000
39	639	0.0385	0.0293	0.0385	0.0293	0.0000	0.0000
657	57	0.0385	0.0261	0.0385	0.0261	0.0000	0.0000
9	609	0.1892	0.1022	0.1892	0.1022	0.0000	0.0000
655	55	0.1892	0.0970	0.1892	0.0970	0.0000	0.0000
1	201	-1.5954	-0.4300	-1.5954	-0.4300	0.0000	0.0000
201	301	-1.5954	-0.4300	-1.5954	-0.4300	0.0000	0.0000
301	401	-1.5954	-0.4300	-1.5954	-0.4300	0.0000	0.0000
401	501	-1.5954	-0.4300	-1.5954	-0.4300	0.0000	0.0000
1	271	-1.5954	-0.4301	-1.5954	-0.4301	0.0000	0.0000
271	371	-1.5954	-0.4301	-1.5954	-0.4301	0.0000	0.0000
371	471	-1.5954	-0.4301	-1.5954	-0.4301	0.0000	0.0000
471	571	-1.5954	-0.4301	-1.5954	-0.4301	0.0000	0.0000
1	281	-1.5954	-0.4300	-1.5954	-0.4300	0.0000	0.0000
281	381	-1.5954	-0.4300	-1.5954	-0.4300	0.0000	0.0000
381	481	-1.5954	-0.4300	-1.5954	-0.4300	0.0000	0.0000
481	581	-1.5954	-0.4300	-1.5954	-0.4300	0.0000	0.0000
3	203	-0.4000	0.0110	-0.4000	0.0110	0.0000	0.0000
203	303	-0.4000	0.0110	-0.4000	0.0110	0.0000	0.0000
303	403	-0.4000	0.0110	-0.4000	0.0110	0.0000	0.0000
403	503	-0.4000	0.0110	-0.4000	0.0110	0.0000	0.0000
8	208	-1.5000	-0.2066	-1.5000	-0.2066	0.0000	0.0000
208	308	-1.5000	-0.2066	-1.5000	-0.2066	0.0000	0.0000
308	408	-1.5000	-0.2066	-1.5000	-0.2066	0.0000	0.0000
408	508	-1.5000	-0.2066	-1.5000	-0.2066	0.0000	0.0000
8	278	-1.5000	-0.2066	-1.5000	-0.2066	0.0000	0.0000
278	378	-1.5000	-0.2066	-1.5000	-0.2066	0.0000	0.0000
378	478	-1.5000	-0.2066	-1.5000	-0.2066	0.0000	0.0000
478	578	-1.5000	-0.2066	-1.5000	-0.2066	0.0000	0.0000
8	288	-1.5000	-0.2067	-1.5000	-0.2067	0.0000	0.0000
288	388	-1.5000	-0.2067	-1.5000	-0.2067	0.0000	0.0000
388	488	-1.5000	-0.2067	-1.5000	-0.2067	0.0000	0.0000
488	588	-1.5000	-0.2067	-1.5000	-0.2067	0.0000	0.0000

Table B.29
Power flow branch solution in IEEE 57-bus system (Part 5)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
12	212	-1.5500	-0.6425	-1.5500	-0.6425	0.0000	0.0000
212	312	-1.5500	-0.6425	-1.5500	-0.6425	0.0000	0.0000
312	412	-1.5500	-0.6425	-1.5500	-0.6425	0.0000	0.0000
412	512	-1.5500	-0.6425	-1.5500	-0.6425	0.0000	0.0000
12	272	-1.5500	-0.6425	-1.5500	-0.6425	0.0000	0.0000
272	372	-1.5500	-0.6425	-1.5500	-0.6425	0.0000	0.0000
372	472	-1.5500	-0.6425	-1.5500	-0.6425	0.0000	0.0000
472	572	-1.5500	-0.6425	-1.5500	-0.6425	0.0000	0.0000
2	202	0.0000	0.0077	0.0000	0.0077	0.0000	0.0000
202	302	0.0000	0.0077	0.0000	0.0077	0.0000	0.0000
302	402	0.0000	0.0077	0.0000	0.0077	0.0000	0.0000
402	502	0.0000	0.0077	0.0000	0.0077	0.0000	0.0000
6	206	0.0000	-0.0071	0.0000	-0.0071	0.0000	0.0000
206	306	0.0000	-0.0071	0.0000	-0.0071	0.0000	0.0000
306	406	0.0000	-0.0071	0.0000	-0.0071	0.0000	0.0000
406	506	0.0000	-0.0071	0.0000	-0.0071	0.0000	0.0000
9	209	0.0000	-0.0193	0.0000	-0.0193	0.0000	0.0000
209	309	0.0000	-0.0193	0.0000	-0.0193	0.0000	0.0000
309	409	0.0000	-0.0193	0.0000	-0.0193	0.0000	0.0000
409	509	0.0000	-0.0193	0.0000	-0.0193	0.0000	0.0000

The total P loss and Q loss are 0.2781 (p.u.) and 0.0611 (p.u.), individually.

Table B.30
System (branch) setting data (Part 1)

From	To	R	X	Y/2	Tap	Remark
1	2	0.00830	0.02800	0.06450	0.00000	
2	3	0.02980	0.08500	0.04090	0.00000	
3	4	0.01120	0.03660	0.01900	0.00000	
4	5	0.06250	0.13200	0.01290	0.00000	
4	6	0.04300	0.14800	0.01740	0.00000	
6	7	0.02000	0.10200	0.01380	0.00000	
6	8	0.03390	0.17300	0.02350	0.00000	
8	9	0.00990	0.05050	0.02740	0.00000	
9	10	0.03690	0.16790	0.02200	0.00000	
9	11	0.02580	0.08480	0.01090	0.00000	
9	12	0.06480	0.29500	0.03860	0.00000	
9	13	0.04810	0.15800	0.02030	0.00000	
13	14	0.01320	0.04340	0.00550	0.00000	
13	15	0.02690	0.08690	0.01150	0.00000	
1	15	0.01780	0.09100	0.04940	0.00000	
1	16	0.04540	0.20600	0.02730	0.00000	
1	17	0.02380	0.10800	0.01430	0.00000	
3	15	0.01620	0.05300	0.02720	0.00000	
5	6	0.03020	0.06410	0.00620	0.00000	
7	8	0.01390	0.07120	0.00970	0.00000	
10	12	0.02770	0.12620	0.01640	0.00000	
11	13	0.02230	0.07320	0.00940	0.00000	
12	13	0.01780	0.05800	0.03020	0.00000	
12	16	0.01800	0.08130	0.01080	0.00000	
12	17	0.03970	0.17900	0.02380	0.00000	
14	15	0.01710	0.05470	0.00740	0.00000	
18	19	0.46100	0.68500	0.00000	0.00000	
19	20	0.28300	0.43400	0.00000	0.00000	
21	22	0.07360	0.11700	0.00000	0.00000	
22	23	0.00990	0.01520	0.00000	0.00000	
23	24	0.16600	0.25600	0.00420	0.00000	
26	27	0.16500	0.25400	0.00000	0.00000	
27	28	0.06180	0.09540	0.00000	0.00000	
28	29	0.04180	0.05870	0.00000	0.00000	
25	30	0.13500	0.20200	0.00000	0.00000	

Table B.31
System (branch) setting data (Part 2)

From	To	R	X	Y/2	Tap	Remark
30	31	0.32600	0.49700	0.00000	0.00000	
31	32	0.50700	0.75500	0.00000	0.00000	
32	33	0.03920	0.03600	0.00000	0.00000	
34	35	0.05200	0.07800	0.00160	0.00000	
35	36	0.04300	0.05370	0.00080	0.00000	
36	37	0.02900	0.03660	0.00000	0.00000	
37	38	0.06510	0.10090	0.00100	0.00000	
37	39	0.02390	0.03790	0.00000	0.00000	
36	40	0.03000	0.04660	0.00000	0.00000	
22	38	0.01920	0.02950	0.00000	0.00000	
41	42	0.20700	0.35200	0.00000	0.00000	
41	43	0.00000	0.41200	0.00000	0.00000	
38	44	0.02890	0.05850	0.00100	0.00000	
46	47	0.02300	0.06800	0.00160	0.00000	
47	48	0.01820	0.02330	0.00000	0.00000	
48	49	0.08340	0.12900	0.00240	0.00000	
49	50	0.08010	0.12800	0.00000	0.00000	
50	51	0.13860	0.22000	0.00000	0.00000	
29	52	0.14420	0.18700	0.00000	0.00000	
52	53	0.07620	0.09840	0.00000	0.00000	
53	54	0.18780	0.23200	0.00000	0.00000	
54	55	0.17320	0.22650	0.00000	0.00000	
44	45	0.06240	0.12420	0.00200	0.00000	
56	41	0.55300	0.54900	0.00000	0.00000	
56	42	0.21250	0.35400	0.00000	0.00000	
57	56	0.17400	0.26000	0.00000	0.00000	
38	49	0.11500	0.17700	0.00150	0.00000	
38	48	0.03120	0.04820	0.00000	0.00000	
604	618	0.00000	0.55500	0.00000	1.03093	
704	718	0.00000	0.43000	0.00000	1.02250	
621	620	0.00000	0.77670	0.00000	0.95877	
624	625	0.00000	1.18200	0.00000	1.00000	
724	725	0.00000	1.23000	0.00000	1.00000	
824	626	0.00000	0.04730	0.00000	0.95877	
607	629	0.00000	0.06480	0.00000	1.03413	

Table B.32
System (branch) setting data (Part 3)

From	To	R	X	Y/2	Tap	Remark
634	632	0.00000	0.95300	0.00000	1.02564	
611	641	0.00000	0.74900	0.00000	1.04712	
615	645	0.00000	0.10420	0.00000	1.04712	
614	646	0.00000	0.07350	0.00000	1.11111	
610	651	0.00000	0.07120	0.00000	1.07527	
613	649	0.00000	0.19100	0.00000	1.11732	
711	643	0.00000	0.15300	0.00000	1.04384	
640	656	0.00000	1.19500	0.00000	1.04384	
639	657	0.00000	1.35500	0.00000	1.02041	
609	655	0.00000	0.12050	0.00000	1.06383	
4	604	0.00000	0.00000	0.00000	0.00000	CB1
618	18	0.00000	0.00000	0.00000	0.00000	CB1
4	704	0.00000	0.00000	0.00000	0.00000	CB1
718	18	0.00000	0.00000	0.00000	0.00000	CB1
21	621	0.00000	0.00000	0.00000	0.00000	CB1
620	20	0.00000	0.00000	0.00000	0.00000	CB1
24	624	0.00000	0.00000	0.00000	0.00000	CB1
625	25	0.00000	0.00000	0.00000	0.00000	CB1
24	724	0.00000	0.00000	0.00000	0.00000	CB1
725	25	0.00000	0.00000	0.00000	0.00000	CB1
24	824	0.00000	0.00000	0.00000	0.00000	CB1
626	26	0.00000	0.00000	0.00000	0.00000	CB1
7	607	0.00000	0.00000	0.00000	0.00000	CB1
629	29	0.00000	0.00000	0.00000	0.00000	CB1
34	634	0.00000	0.00000	0.00000	0.00000	CB1
632	32	0.00000	0.00000	0.00000	0.00000	CB1
11	611	0.00000	0.00000	0.00000	0.00000	CB1
641	41	0.00000	0.00000	0.00000	0.00000	CB1
15	615	0.00000	0.00000	0.00000	0.00000	CB1
645	45	0.00000	0.00000	0.00000	0.00000	CB1
14	614	0.00000	0.00000	0.00000	0.00000	CB1
646	46	0.00000	0.00000	0.00000	0.00000	CB1
10	610	0.00000	0.00000	0.00000	0.00000	CB1
651	51	0.00000	0.00000	0.00000	0.00000	CB1
13	613	0.00000	0.00000	0.00000	0.00000	CB1

Table B.33
System (branch) setting data (Part 4)

From	To	R	X	Y/2	Tap	Remark
649	49	0.00000	0.00000	0.00000	0.00000	CB1
11	711	0.00000	0.00000	0.00000	0.00000	CB1
643	43	0.00000	0.00000	0.00000	0.00000	CB1
40	640	0.00000	0.00000	0.00000	0.00000	CB1
656	56	0.00000	0.00000	0.00000	0.00000	CB1
39	639	0.00000	0.00000	0.00000	0.00000	CB1
657	57	0.00000	0.00000	0.00000	0.00000	CB1
9	609	0.00000	0.00000	0.00000	0.00000	CB1
655	55	0.00000	0.00000	0.00000	0.00000	CB1
1	201	0.00000	0.00000	0.00000	0.00000	CB1
201	301	0.00000	0.00000	0.00000	0.00000	CB1
301	401	0.00000	0.00000	0.00000	0.00000	CB1
401	501	0.00000	0.00000	0.00000	0.00000	CB1
1	271	0.00000	0.00000	0.00000	0.00000	CB1
271	371	0.00000	0.00000	0.00000	0.00000	CB1
371	471	0.00000	0.00000	0.00000	0.00000	CB1
471	571	0.00000	0.00000	0.00000	0.00000	CB1
1	281	0.00000	0.00000	0.00000	0.00000	CB1
281	381	0.00000	0.00000	0.00000	0.00000	CB1
381	481	0.00000	0.00000	0.00000	0.00000	CB1
481	581	0.00000	0.00000	0.00000	0.00000	CB1
3	203	0.00000	0.00000	0.00000	0.00000	CB1
203	303	0.00000	0.00000	0.00000	0.00000	CB1
303	403	0.00000	0.00000	0.00000	0.00000	CB1
403	503	0.00000	0.00000	0.00000	0.00000	CB1
8	208	0.00000	0.00000	0.00000	0.00000	CB1
208	308	0.00000	0.00000	0.00000	0.00000	CB1
308	408	0.00000	0.00000	0.00000	0.00000	CB1
408	508	0.00000	0.00000	0.00000	0.00000	CB1
8	278	0.00000	0.00000	0.00000	0.00000	CB1
278	378	0.00000	0.00000	0.00000	0.00000	CB1
378	478	0.00000	0.00000	0.00000	0.00000	CB1
478	578	0.00000	0.00000	0.00000	0.00000	CB1
8	288	0.00000	0.00000	0.00000	0.00000	CB1
288	388	0.00000	0.00000	0.00000	0.00000	CB1

Table B.34
System (branch) setting data (Part 5)

From	To	R	X	Y/2	Tap	Remark
388	488	0.00000	0.00000	0.00000	0.00000	CB1
488	588	0.00000	0.00000	0.00000	0.00000	CB1
12	212	0.00000	0.00000	0.00000	0.00000	CB1
212	312	0.00000	0.00000	0.00000	0.00000	CB1
312	412	0.00000	0.00000	0.00000	0.00000	CB1
412	512	0.00000	0.00000	0.00000	0.00000	CB1
12	272	0.00000	0.00000	0.00000	0.00000	CB1
272	372	0.00000	0.00000	0.00000	0.00000	CB1
372	472	0.00000	0.00000	0.00000	0.00000	CB1
472	572	0.00000	0.00000	0.00000	0.00000	CB1
2	202	0.00000	0.00000	0.00000	0.00000	CB1
202	302	0.00000	0.00000	0.00000	0.00000	CB1
302	402	0.00000	0.00000	0.00000	0.00000	CB1
402	502	0.00000	0.00000	0.00000	0.00000	CB1
6	206	0.00000	0.00000	0.00000	0.00000	CB1
206	306	0.00000	0.00000	0.00000	0.00000	CB1
306	406	0.00000	0.00000	0.00000	0.00000	CB1
406	506	0.00000	0.00000	0.00000	0.00000	CB1
9	209	0.00000	0.00000	0.00000	0.00000	CB1
209	309	0.00000	0.00000	0.00000	0.00000	CB1
309	409	0.00000	0.00000	0.00000	0.00000	CB1
409	509	0.00000	0.00000	0.00000	0.00000	CB1

Table B.35
Power flow condition setting data (Part 1)

Node	V magnitude	PG	QG	PL	QL	QC	Name
1	0.0000	0.0000	0.0000	0.5500	0.1700	0.0000	Kanawha1
2	0.0000	0.0000	0.0000	0.0300	0.8800	0.0000	Turner1
3	0.0000	0.0000	0.0000	0.4100	0.2100	0.0000	Logan1
4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Sprigg
5	0.0000	0.0000	0.0000	0.1300	0.0400	0.0000	Bus5
6	0.0000	0.0000	0.0000	0.7500	0.0200	0.0000	BeaverCk1
7	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus7
8	0.0000	0.0000	0.0000	1.5000	0.2200	0.0000	ClinchRv1
9	0.0000	0.0000	0.0000	1.2100	0.2600	0.0000	Saltville1
10	0.0000	0.0000	0.0000	0.0500	0.0200	0.0000	Bus10
11	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Tazewell
12	0.0000	0.0000	0.0000	3.7700	0.2400	0.0000	Glen Lyn1
13	0.0000	0.0000	0.0000	0.1800	0.0230	0.0000	Bus13
14	0.0000	0.0000	0.0000	0.1050	0.0530	0.0000	Bus14
15	0.0000	0.0000	0.0000	0.2200	0.0500	0.0000	Bus15
16	0.0000	0.0000	0.0000	0.4300	0.0300	0.0000	Bus16
17	0.0000	0.0000	0.0000	0.4200	0.0800	0.0000	Bus17
18	0.0000	0.0000	0.0000	0.2720	0.0980	0.0998	Sprigg
19	0.0000	0.0000	0.0000	0.0330	0.0060	0.0000	Bus19
20	0.0000	0.0000	0.0000	0.0230	0.0100	0.0000	Bus20
21	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus21
22	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus22
23	0.0000	0.0000	0.0000	0.0630	0.0210	0.0000	Bus23
24	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus24
25	0.0000	0.0000	0.0000	0.0630	0.0320	0.0612	Bus25
26	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus26
27	0.0000	0.0000	0.0000	0.0930	0.0050	0.0000	Bus27
28	0.0000	0.0000	0.0000	0.0460	0.0230	0.0000	Bus28
29	0.0000	0.0000	0.0000	0.1700	0.0260	0.0000	Bus29
30	0.0000	0.0000	0.0000	0.0360	0.0180	0.0000	Bus30
31	0.0000	0.0000	0.0000	0.0580	0.0290	0.0000	Bus31
32	0.0000	0.0000	0.0000	0.0160	0.0080	0.0000	Bus32
33	0.0000	0.0000	0.0000	0.0380	0.0190	0.0000	Bus33
34	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus34
35	0.0000	0.0000	0.0000	0.0600	0.0300	0.0000	Bus35

Table B.36
Power flow condition setting data (Part 2)

Node	V magnitude	PG	QG	PL	QL	QC	Name
36	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus36
37	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus37
38	0.0000	0.0000	0.0000	0.1400	0.0700	0.0000	Bus38
39	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus39
40	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus40
41	0.0000	0.0000	0.0000	0.0630	0.0300	0.0000	Tazewell
42	0.0000	0.0000	0.0000	0.0710	0.0440	0.0000	Bus42
43	0.0000	0.0000	0.0000	0.0200	0.0100	0.0000	Tazewell
44	0.0000	0.0000	0.0000	0.1200	0.0180	0.0000	Bus44
45	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus45
46	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus46
47	0.0000	0.0000	0.0000	0.2970	0.1160	0.0000	Bus47
48	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Bus48
49	0.0000	0.0000	0.0000	0.1800	0.0850	0.0000	Bus49
50	0.0000	0.0000	0.0000	0.2100	0.1050	0.0000	Bus50
51	0.0000	0.0000	0.0000	0.1800	0.0530	0.0000	Bus51
52	0.0000	0.0000	0.0000	0.0490	0.0220	0.0000	Bus52
53	0.0000	0.0000	0.0000	0.2000	0.1000	0.0668	Bus53
54	0.0000	0.0000	0.0000	0.0410	0.0140	0.0000	Bus54
55	0.0000	0.0000	0.0000	0.0680	0.0340	0.0000	Saltville
56	0.0000	0.0000	0.0000	0.0760	0.0220	0.0000	Bus56
57	0.0000	0.0000	0.0000	0.0670	0.0200	0.0000	Bus57
58	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Kanawha2A
59	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Turner2
60	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Logan2
61	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	BeaverCk2
62	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	ClinchRv2A
63	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Saltville2
64	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Glen Lyn2A
65	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Kanawha2B
66	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Glen Lyn2B
67	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	ClinchRv2B
68	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Kanawha2C
69	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	ClinchRv2C
70	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.37
Power flow condition setting data (Part 3)

Node	V magnitude	PG	QG	PL	QL	QC	Name
71	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
72	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
73	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
74	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
75	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
76	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
77	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
78	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
79	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
80	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
81	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
82	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
83	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
84	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
85	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
86	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
87	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
88	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
89	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
90	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
91	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
92	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
93	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
94	1.0400	0.0000	0.0000	0.0000	0.0000	0.0000	
95	1.0100	0.0000	-0.0080	0.0000	0.0000	0.0000	
96	0.9850	0.4000	0.0000	0.0000	0.0000	0.0000	
97	0.9800	0.0000	0.0080	0.0000	0.0000	0.0000	
98	1.0050	1.5000	0.0000	0.0000	0.0000	0.0000	
99	0.9800	0.0000	0.0220	0.0000	0.0000	0.0000	
100	1.0150	1.5500	0.0000	0.0000	0.0000	0.0000	
101	1.0400	1.5954	0.0000	0.0000	0.0000	0.0000	
102	1.0150	1.5500	0.0000	0.0000	0.0000	0.0000	
103	1.0050	1.5000	0.0000	0.0000	0.0000	0.0000	
104	1.0400	1.5954	0.0000	0.0000	0.0000	0.0000	
105	1.0050	1.5000	0.0000	0.0000	0.0000	0.0000	

Table B.38
Power flow condition setting data (Part 4)

Node	V magnitude	PG	QG	PL	QL	QC	Name
106	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
107	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
108	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
109	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
110	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
111	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
112	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
113	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
114	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
115	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
116	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
117	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
118	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
119	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
120	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
121	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
122	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
123	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
124	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
125	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
126	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
127	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
128	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
129	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
130	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
131	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
132	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
133	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
134	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
135	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
136	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
137	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
138	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
139	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.39
Generator constants with implemented generator controller

Node	AVR	OEL	PSS	GOV	GVA	GMW	GPF	MG	DG	PLM	Name
501	X	X		X	182	170	0.934	6.0	0.0	5.0	G1A
571	X	X		X	182	170	0.934	6.0	0.0	5.0	G1B
581	X	X		X	182	170	0.934	6.0	0.0	5.0	G1C
503	X	X		X	100	80	0.800	6.0	0.0	5.0	G3
508	X	X		X	182	170	0.934	6.0	0.0	5.0	G8A
578	X	X		X	182	170	0.934	6.0	0.0	5.0	G8B
588	X	X		X	182	170	0.934	6.0	0.0	5.0	G8C
512	X	X		X	178	160	0.899	6.0	0.0	5.0	G12A
572	X	X		X	178	160	0.899	6.0	0.0	5.0	G12B
502	X				50	0	0.000	1.5	0.0	0.0	C2
506	X				25	0	0.000	1.5	0.0	0.0	C6
509	X				9	0	0.000	1.5	0.0	0.0	C9

Table B.40
Generator constants of the used generator model

Node	RA	XL	XD	XDD	XDDD	XFLD	XKLD	XQ	XQDD	XKLQ	TDD	TDDD	RFD	RKD	TQDD	RKQ
501	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
571	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
581	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
503	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
508	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
578	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
588	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
512	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
572	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
502	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
506	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
509	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195

Table B.41
Initial condition of synchronous generator and condenser

Node	AGG	VT	PG	QG	TQG	EF	CF	CDD	CQQ	FGD	FGQ
501	45.10	1.0400	0.8766	0.2363	0.8779	2.0224	2.0224	0.7574	0.4341	0.9053	-0.6402
571	45.10	1.0400	0.8766	0.2363	0.8778	2.0225	2.0225	0.7574	0.4340	0.9053	-0.6402
581	45.10	1.0400	0.8766	0.2363	0.8778	2.0224	2.0224	0.7574	0.4341	0.9053	-0.6402
503	29.56	0.9850	0.4000	-0.0110	0.4003	1.1879	1.1879	0.2269	0.3370	0.8532	-0.4970
508	44.84	1.0050	0.8242	0.1135	0.8253	1.8383	1.8383	0.6955	0.4490	0.8124	-0.6622
578	44.84	1.0050	0.8242	0.1135	0.8253	1.8383	1.8383	0.6955	0.4490	0.8124	-0.6622
588	44.84	1.0050	0.8242	0.1136	0.8253	1.8383	1.8383	0.6955	0.4490	0.8124	-0.6622
512	31.51	1.0150	0.8708	0.3610	0.8722	2.1802	2.1802	0.8381	0.4001	0.9439	-0.5901
572	31.51	1.0150	0.8708	0.3610	0.8722	2.1801	2.1801	0.8381	0.4001	0.9439	-0.5901
502	-1.19	1.0100	0.0000	-0.0155	0.0000	0.9840	0.9840	0.0153	0.0000	1.0066	0.0000
506	-8.66	0.9800	0.0000	0.0282	0.0000	1.0289	1.0289	0.0288	0.0000	0.9865	0.0000
509	-9.59	0.9800	0.0000	0.2145	0.0001	1.3521	1.3521	0.2189	0.0001	1.0292	-0.0001

B.4 IEEE 118-bus System

The system diagram is shown in Fig. B.5. Power flow solutions are summarized in Tables B.42, B.43, B.43, and B.45. The system MVA is 100 MVA. The power flow setting data are also provided in Tables B.64, B.65, B.66, B.67, B.68, B.76, B.77 and B.78. It is noted that circuit breakers with no impedance are inserted between the main grid and individual power equipment.

Initial conditions of the dynamic simulation with generator constants are sorted out in Tables B.86, B.87, B.88, B.89, B.90 and B.91.

It is noted that the generator's saturation characteristics is used for the IEEE 118-bus systems (Fig. B.3).

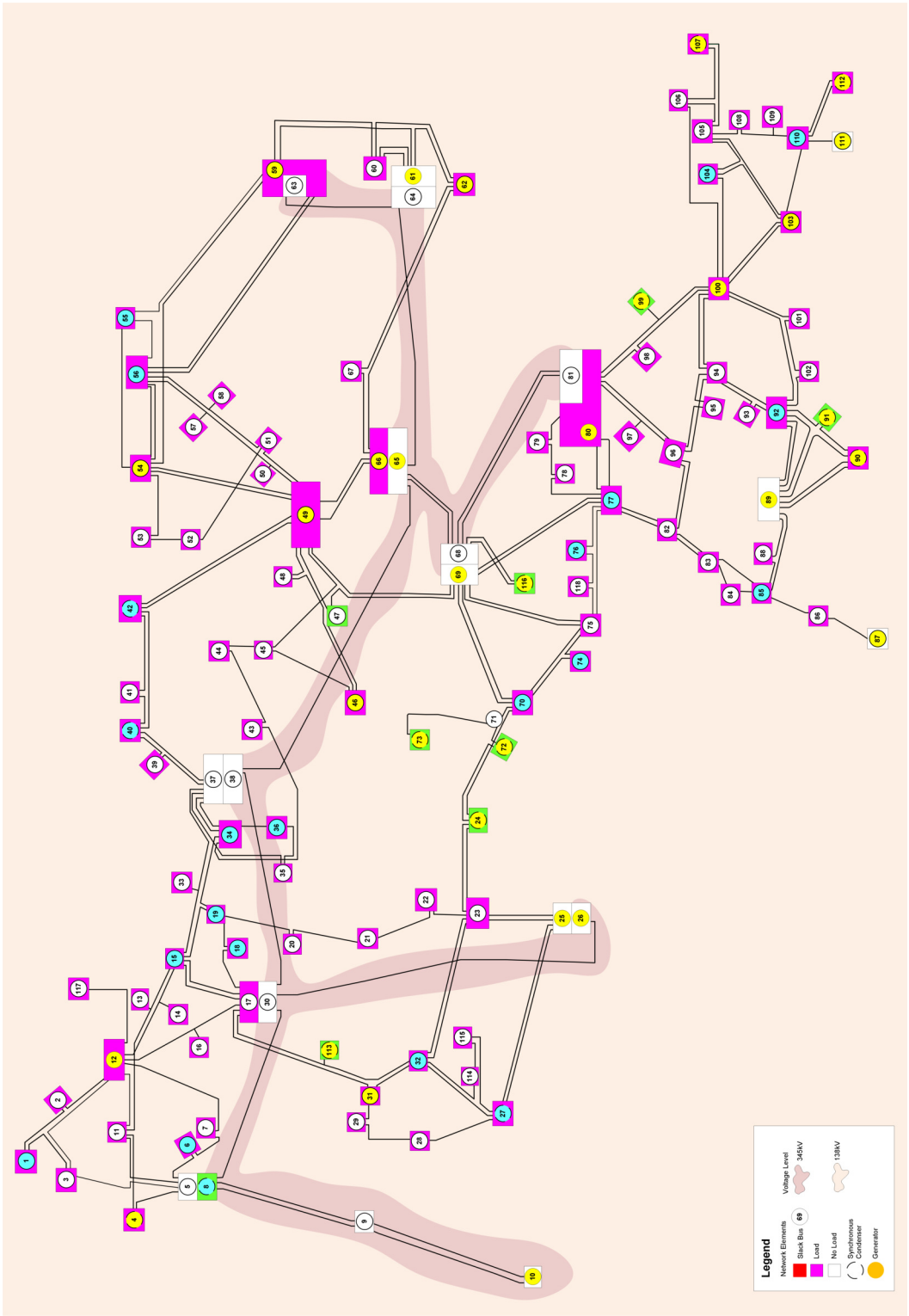


Figure B.5: Diagram of IEEE 118-bus system

Table B.42
Power flow node solution in IEEE 118-bus system (part 1)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
1	0.9550	-19.16	0.0000	0.0000	0.5100	0.2700	0.0000	Riverside1
2	0.9714	-18.63	0.0000	0.0000	0.2000	0.0900	0.0000	Pokagon
3	0.9677	-18.27	0.0000	0.0000	0.3900	0.1000	0.0000	HickoryCk
4	0.9980	-14.54	0.0000	0.0000	0.3900	0.1200	0.0000	NCarlisle1
5	1.0018	-14.09	0.0000	0.0000	0.0000	0.0000	-0.4015	Olive
6	0.9900	-16.84	0.0000	0.0000	0.5200	0.2200	0.0000	Kankakee1
7	0.9893	-17.29	0.0000	0.0000	0.1900	0.0200	0.0000	JacksonRd
8	1.0150	-8.88	0.0000	0.0000	0.2800	0.0000	0.0000	Olive1
9	1.0430	-1.67	0.0000	0.0000	0.0000	0.0000	0.0000	Beguine
10	1.0500	5.86	0.0000	0.0000	0.0000	0.0000	0.0000	Breed1
11	0.9850	-17.13	0.0000	0.0000	0.7000	0.2300	0.0000	SouthBend
12	0.9900	-17.66	0.0000	0.0000	0.4700	0.1000	0.0000	TwnBranch1
13	0.9683	-18.54	0.0000	0.0000	0.3400	0.1600	0.0000	Concord
14	0.9836	-18.41	0.0000	0.0000	0.1400	0.0100	0.0000	GoshenJct
15	0.9700	-18.79	0.0000	0.0000	0.9000	0.3000	0.0000	FortWayne1
16	0.9838	-17.99	0.0000	0.0000	0.2500	0.1000	0.0000	N. E.
17	0.9948	-16.26	0.0000	0.0000	0.1100	0.0300	0.0000	Sorenson
18	0.9730	-18.49	0.0000	0.0000	0.6000	0.3400	0.0000	McKinley1
19	0.9620	-18.96	0.0000	0.0000	0.4500	0.2500	0.0000	Lincoln1
20	0.9569	-18.06	0.0000	0.0000	0.1800	0.0300	0.0000	Adams
21	0.9577	-16.45	0.0000	0.0000	0.1400	0.0800	0.0000	Jay
22	0.9690	-13.88	0.0000	0.0000	0.1000	0.0500	0.0000	Randolph
23	0.9994	-8.93	0.0000	0.0000	0.0700	0.0300	0.0000	CollgeCnr
24	0.9920	-9.03	0.0000	0.0000	0.1300	0.0000	0.0000	Trenton1
25	1.0500	-2.01	0.0000	0.0000	0.0000	0.0000	0.0000	TannersCk1
26	1.0150	-0.07	0.0000	0.0000	0.0000	0.0000	0.0000	TannersCk3
27	0.9680	-14.58	0.0000	0.0000	0.7100	0.1300	0.0000	Madison1
28	0.9616	-16.32	0.0000	0.0000	0.1700	0.0700	0.0000	Mullin
29	0.9632	-17.32	0.0000	0.0000	0.2400	0.0400	0.0000	Grant
30	0.9871	-10.83	0.0000	0.0000	0.0000	0.0000	0.0000	Sorenson
31	0.9670	-17.21	0.0000	0.0000	0.4300	0.2700	0.0000	DeerCreek1
32	0.9630	-15.13	0.0000	0.0000	0.5900	0.2300	0.0000	Delaware1
33	0.9707	-19.50	0.0000	0.0000	0.2300	0.0900	0.0000	Haviland
34	0.9840	-18.93	0.0000	0.0000	0.5900	0.2600	0.1356	Rockhill1
35	0.9804	-19.39	0.0000	0.0000	0.3300	0.0900	0.0000	West Lima
36	0.9800	-19.39	0.0000	0.0000	0.3100	0.1700	0.0000	Sterling1
37	0.9902	-18.48	0.0000	0.0000	0.0000	0.0000	-0.2451	East Lima

Table B.43
Power flow node solution in IEEE 118-bus system (part 2)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
38	0.9645	-12.71	0.0000	0.0000	0.0000	0.0000	0.0000	East Lima
39	0.9698	-21.83	0.0000	0.0000	0.2700	0.1100	0.0000	NwLiberty
40	0.9700	-22.88	0.0000	0.0000	0.6600	0.2300	0.0000	West End1
41	0.9668	-23.31	0.0000	0.0000	0.3700	0.1000	0.0000	S. Tiffin
42	0.9850	-21.65	0.0000	0.0000	0.9600	0.2300	0.0000	Howard1
43	0.9771	-18.92	0.0000	0.0000	0.1800	0.0700	0.0000	S. Kenton
44	0.9843	-16.35	0.0000	0.0000	0.1600	0.0800	0.0969	WMtVernon
45	0.9863	-14.49	0.0000	0.0000	0.5300	0.2200	0.0973	N. Newark
46	1.0050	-11.65	0.0000	0.0000	0.2800	0.1000	0.1010	W.Lancstr1
47	1.0170	-9.40	0.0000	0.0000	0.3400	0.0000	0.0000	Crooksvil
48	1.0206	-10.22	0.0000	0.0000	0.2000	0.1100	0.1563	Zanesvile
49	1.0250	-9.21	0.0000	0.0000	0.8700	0.3000	0.0000	Philo1
50	1.0011	-11.26	0.0000	0.0000	0.1700	0.0400	0.0000	W.Cambrdg
51	0.9669	-13.89	0.0000	0.0000	0.1700	0.0800	0.0000	Newcmrstn
52	0.9568	-14.85	0.0000	0.0000	0.1800	0.0500	0.0000	SCoshoctn
53	0.9460	-15.83	0.0000	0.0000	0.2300	0.1100	0.0000	Wooster
54	0.9550	-14.93	0.0000	0.0000	1.1300	0.3200	0.0000	Torrey1
55	0.9520	-15.22	0.0000	0.0000	0.6300	0.2200	0.0000	Wagenhals1
56	0.9540	-15.03	0.0000	0.0000	0.8400	0.1800	0.0000	Sunnyside1
57	0.9706	-13.81	0.0000	0.0000	0.1200	0.0300	0.0000	WNwPhila1
58	0.9590	-14.67	0.0000	0.0000	0.1200	0.0300	0.0000	WNwPhila2
59	0.9850	-10.88	0.0000	0.0000	2.7700	1.1300	0.0000	Tidd1
60	0.9931	-7.00	0.0000	0.0000	0.7800	0.0300	0.0000	SW Kammer
61	0.9950	-6.10	0.0000	0.0000	0.0000	0.0000	0.0000	W. Kammer1
62	0.9980	-6.72	0.0000	0.0000	0.7700	0.1400	0.0000	Natrium1
63	0.9698	-7.30	0.0000	0.0000	0.0000	0.0000	0.0000	Tidd
64	0.9842	-5.58	0.0000	0.0000	0.0000	0.0000	0.0000	Kammer
65	1.0050	-2.48	0.0000	0.0000	0.0000	0.0000	0.0000	Muskingum1
66	1.0500	-2.67	0.0000	0.0000	0.3900	0.1800	0.0000	Muskingum1
67	1.0197	-5.31	0.0000	0.0000	0.2800	0.0700	0.0000	Summerfld
68	1.0038	-2.63	0.0000	0.0000	0.0000	0.0000	0.0000	Sporn
69	1.0350	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	Sporn1
70	0.9840	-7.42	0.0000	0.0000	0.6600	0.2000	0.0000	Portsmoth1
71	0.9868	-7.84	0.0000	0.0000	0.0000	0.0000	0.0000	NPortsmth
72	0.9800	-8.99	0.0000	0.0000	0.1200	0.0000	0.0000	Hillsboro1
73	0.9910	-8.05	0.0000	0.0000	0.0600	0.0000	0.0000	Sargents1
74	0.9580	-8.36	0.0000	0.0000	0.6800	0.2700	0.1101	Bellefont1

Table B.44
Power flow node solution in IEEE 118-bus system (part 3)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
75	0.9674	-7.09	0.0000	0.0000	0.4700	0.1100	0.0000	Sth Point
76	0.9430	-8.24	0.0000	0.0000	0.6800	0.3600	0.0000	Darrah1
77	1.0060	-3.30	0.0000	0.0000	0.6100	0.2800	0.0000	Turner1
78	1.0034	-3.61	0.0000	0.0000	0.7100	0.2600	0.0000	Chemical
79	1.0092	-3.32	0.0000	0.0000	0.3900	0.3200	0.2037	CapitolHl
80	1.0400	-1.08	0.0000	0.0000	1.3000	0.2600	0.0000	Cabin Crk1
81	0.9984	-2.08	0.0000	0.0000	0.0000	0.0000	0.0000	Kanawha
82	0.9886	-2.79	0.0000	0.0000	0.5400	0.2700	0.1955	Logan
83	0.9844	-1.60	0.0000	0.0000	0.2000	0.1000	0.0969	Sprigg
84	0.9797	0.93	0.0000	0.0000	0.1100	0.0700	0.0000	BetsyLayn
85	0.9850	2.49	0.0000	0.0000	0.2400	0.1500	0.0000	BeaverCrk1
86	0.9867	1.12	0.0000	0.0000	0.2100	0.1000	0.0000	Hazard
87	1.0150	1.38	0.0000	0.0000	0.0000	0.0000	0.0000	Pineville1
88	0.9875	5.62	0.0000	0.0000	0.4800	0.1000	0.0000	Fremont
89	1.0050	9.67	0.0000	0.0000	0.0000	0.0000	0.0000	ClinchRvr1
90	0.9850	3.27	0.0000	0.0000	1.6300	0.4200	0.0000	Holston1
91	0.9800	3.28	0.0000	0.0000	0.1000	0.0000	0.0000	HolstonTP1
92	0.9900	3.81	0.0000	0.0000	0.6500	0.1000	0.0000	Saltville1
93	0.9854	0.78	0.0000	0.0000	0.1200	0.0700	0.0000	Tazewell
94	0.9899	-1.38	0.0000	0.0000	0.3000	0.1600	0.0000	Switchbak
95	0.9804	-2.36	0.0000	0.0000	0.4200	0.3100	0.0000	Caldwell
96	0.9923	-2.52	0.0000	0.0000	0.3800	0.1500	0.0000	Baileysvl
97	1.0112	-2.15	0.0000	0.0000	0.1500	0.0900	0.0000	Sundial
98	1.0235	-2.64	0.0000	0.0000	0.3400	0.0800	0.0000	Bradley
99	1.0100	-3.00	0.0000	0.0000	0.4200	0.0000	0.0000	Hinton1
100	1.0170	-2.01	0.0000	0.0000	0.3700	0.1800	0.0000	Glen Lyn1
101	0.9914	-0.42	0.0000	0.0000	0.2200	0.1500	0.0000	Wythe
102	0.9891	2.29	0.0000	0.0000	0.0500	0.0300	0.0000	Smyth
103	1.0100	-5.74	0.0000	0.0000	0.2300	0.1600	0.0000	Claytor1
104	0.9710	-8.31	0.0000	0.0000	0.3800	0.2500	0.0000	Hancock1
105	0.9650	-9.41	0.0000	0.0000	0.3100	0.2600	0.1862	Roanoke1
106	0.9612	-9.67	0.0000	0.0000	0.4300	0.1600	0.0000	Cloverdle
107	0.9520	-12.47	0.0000	0.0000	0.5000	0.1200	0.0544	Reusens1
108	0.9662	-10.61	0.0000	0.0000	0.0200	0.0100	0.0000	Blaine
109	0.9670	-11.06	0.0000	0.0000	0.0800	0.0300	0.0000	Franklin
110	0.9730	-11.91	0.0000	0.0000	0.3900	0.3000	0.0568	Fieldale1
111	0.9800	-10.26	0.0000	0.0000	0.0000	0.0000	0.0000	Dan River1

Table B.45
Power flow node solution in IEEE 118-bus system (part 4)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
112	0.9750	-15.01	0.0000	0.0000	0.6800	0.1300	0.0000	Danville1
113	0.9930	-16.26	0.0000	0.0000	0.0600	0.0000	0.0000	DeerCk TP1
114	0.9601	-15.46	0.0000	0.0000	0.0800	0.0300	0.0000	W Medford
115	0.9600	-15.47	0.0000	0.0000	0.2200	0.0700	0.0000	Medford
116	1.0050	-3.07	0.0000	0.0000	1.8400	0.0000	0.0000	Kyger Crk1
117	0.9738	-19.20	0.0000	0.0000	0.2000	0.0800	0.0000	Corey
118	0.9495	-8.09	0.0000	0.0000	0.3300	0.1500	0.0000	WHuntngdn
120	1.0018	-14.09	0.0000	0.0000	0.0000	0.0000	0.0000	
123	1.0150	-8.88	0.0000	0.0000	0.0000	0.0000	0.0000	
132	0.9948	-16.26	0.0000	0.0000	0.0000	0.0000	0.0000	
140	1.0500	-2.01	0.0000	0.0000	0.0000	0.0000	0.0000	
141	1.0150	-0.07	0.0000	0.0000	0.0000	0.0000	0.0000	
145	0.9871	-10.83	0.0000	0.0000	0.0000	0.0000	0.0000	
152	0.9902	-18.48	0.0000	0.0000	0.0000	0.0000	0.0000	
153	0.9645	-12.71	0.0000	0.0000	0.0000	0.0000	0.0000	
174	0.9850	-10.88	0.0000	0.0000	0.0000	0.0000	0.0000	
176	0.9950	-6.10	0.0000	0.0000	0.0000	0.0000	0.0000	
178	0.9698	-7.30	0.0000	0.0000	0.0000	0.0000	0.0000	
179	0.9842	-5.58	0.0000	0.0000	0.0000	0.0000	0.0000	
180	1.0050	-2.48	0.0000	0.0000	0.0000	0.0000	0.0000	
181	1.0500	-2.67	0.0000	0.0000	0.0000	0.0000	0.0000	
183	1.0038	-2.63	0.0000	0.0000	0.0000	0.0000	0.0000	
184	1.0350	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
195	1.0400	-1.08	0.0000	0.0000	0.0000	0.0000	0.0000	
196	0.9984	-2.08	0.0000	0.0000	0.0000	0.0000	0.0000	
201	0.9550	-19.16	0.0000	0.0000	0.0000	0.0000	0.0000	
204	0.9980	-14.54	0.0000	0.0000	0.0000	0.0000	0.0000	
206	0.9900	-16.84	0.0000	0.0000	0.0000	0.0000	0.0000	
208	1.0150	-8.88	0.0000	0.0000	0.0000	0.0000	0.0000	
210	1.0500	5.86	0.0000	0.0000	0.0000	0.0000	0.0000	
212	0.9900	-17.66	0.0000	0.0000	0.0000	0.0000	0.0000	
215	0.9700	-18.79	0.0000	0.0000	0.0000	0.0000	0.0000	
218	0.9730	-18.49	0.0000	0.0000	0.0000	0.0000	0.0000	
219	0.9620	-18.96	0.0000	0.0000	0.0000	0.0000	0.0000	
224	0.9920	-9.03	0.0000	0.0000	0.0000	0.0000	0.0000	
225	1.0500	-2.01	0.0000	0.0000	0.0000	0.0000	0.0000	
226	1.0150	-0.07	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.46
Power flow node solution in IEEE 118-bus system (part 5)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
227	0.9680	-14.58	0.0000	0.0000	0.0000	0.0000	0.0000	
231	0.9670	-17.21	0.0000	0.0000	0.0000	0.0000	0.0000	
232	0.9630	-15.13	0.0000	0.0000	0.0000	0.0000	0.0000	
234	0.9840	-18.93	0.0000	0.0000	0.0000	0.0000	0.0000	
236	0.9800	-19.39	0.0000	0.0000	0.0000	0.0000	0.0000	
240	0.9700	-22.88	0.0000	0.0000	0.0000	0.0000	0.0000	
242	0.9850	-21.65	0.0000	0.0000	0.0000	0.0000	0.0000	
246	1.0050	-11.65	0.0000	0.0000	0.0000	0.0000	0.0000	
249	1.0250	-9.21	0.0000	0.0000	0.0000	0.0000	0.0000	
254	0.9550	-14.93	0.0000	0.0000	0.0000	0.0000	0.0000	
255	0.9520	-15.22	0.0000	0.0000	0.0000	0.0000	0.0000	
256	0.9540	-15.03	0.0000	0.0000	0.0000	0.0000	0.0000	
259	0.9850	-10.88	0.0000	0.0000	0.0000	0.0000	0.0000	
261	0.9950	-6.10	0.0000	0.0000	0.0000	0.0000	0.0000	
262	0.9980	-6.72	0.0000	0.0000	0.0000	0.0000	0.0000	
265	1.0050	-2.48	0.0000	0.0000	0.0000	0.0000	0.0000	
266	1.0500	-2.67	0.0000	0.0000	0.0000	0.0000	0.0000	
269	1.0350	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
270	0.9840	-7.42	0.0000	0.0000	0.0000	0.0000	0.0000	
272	0.9800	-8.99	0.0000	0.0000	0.0000	0.0000	0.0000	
273	0.9910	-8.05	0.0000	0.0000	0.0000	0.0000	0.0000	
274	0.9580	-8.36	0.0000	0.0000	0.0000	0.0000	0.0000	
276	0.9430	-8.24	0.0000	0.0000	0.0000	0.0000	0.0000	
277	1.0060	-3.30	0.0000	0.0000	0.0000	0.0000	0.0000	
280	1.0400	-1.08	0.0000	0.0000	0.0000	0.0000	0.0000	
285	0.9850	2.49	0.0000	0.0000	0.0000	0.0000	0.0000	
287	1.0150	1.38	0.0000	0.0000	0.0000	0.0000	0.0000	
289	1.0050	9.67	0.0000	0.0000	0.0000	0.0000	0.0000	
290	0.9850	3.27	0.0000	0.0000	0.0000	0.0000	0.0000	
291	0.9800	3.28	0.0000	0.0000	0.0000	0.0000	0.0000	
292	0.9900	3.81	0.0000	0.0000	0.0000	0.0000	0.0000	
299	1.0100	-3.00	0.0000	0.0000	0.0000	0.0000	0.0000	
301	0.9550	-19.16	0.0000	0.0000	0.0000	0.0000	0.0000	
304	0.9980	-14.54	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.47
Power flow node solution in IEEE 118-bus system (part 6)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
306	0.9900	-16.84	0.0000	0.0000	0.0000	0.0000	0.0000	
308	1.0150	-8.88	0.0000	0.0000	0.0000	0.0000	0.0000	
310	1.0500	5.86	0.0000	0.0000	0.0000	0.0000	0.0000	
312	0.9900	-17.66	0.0000	0.0000	0.0000	0.0000	0.0000	
315	0.9700	-18.79	0.0000	0.0000	0.0000	0.0000	0.0000	
318	0.9730	-18.49	0.0000	0.0000	0.0000	0.0000	0.0000	
319	0.9620	-18.96	0.0000	0.0000	0.0000	0.0000	0.0000	
324	0.9920	-9.03	0.0000	0.0000	0.0000	0.0000	0.0000	
325	1.0500	-2.01	0.0000	0.0000	0.0000	0.0000	0.0000	
326	1.0150	-0.07	0.0000	0.0000	0.0000	0.0000	0.0000	
327	0.9680	-14.58	0.0000	0.0000	0.0000	0.0000	0.0000	
331	0.9670	-17.21	0.0000	0.0000	0.0000	0.0000	0.0000	
332	0.9630	-15.13	0.0000	0.0000	0.0000	0.0000	0.0000	
334	0.9840	-18.93	0.0000	0.0000	0.0000	0.0000	0.0000	
336	0.9800	-19.39	0.0000	0.0000	0.0000	0.0000	0.0000	
340	0.9700	-22.88	0.0000	0.0000	0.0000	0.0000	0.0000	
342	0.9850	-21.65	0.0000	0.0000	0.0000	0.0000	0.0000	
346	1.0050	-11.65	0.0000	0.0000	0.0000	0.0000	0.0000	
349	1.0250	-9.21	0.0000	0.0000	0.0000	0.0000	0.0000	
354	0.9550	-14.93	0.0000	0.0000	0.0000	0.0000	0.0000	
355	0.9520	-15.22	0.0000	0.0000	0.0000	0.0000	0.0000	
356	0.9540	-15.03	0.0000	0.0000	0.0000	0.0000	0.0000	
359	0.9850	-10.88	0.0000	0.0000	0.0000	0.0000	0.0000	
361	0.9950	-6.10	0.0000	0.0000	0.0000	0.0000	0.0000	
362	0.9980	-6.72	0.0000	0.0000	0.0000	0.0000	0.0000	
365	1.0050	-2.48	0.0000	0.0000	0.0000	0.0000	0.0000	
366	1.0500	-2.67	0.0000	0.0000	0.0000	0.0000	0.0000	
369	1.0350	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
370	0.9840	-7.42	0.0000	0.0000	0.0000	0.0000	0.0000	
372	0.9800	-8.99	0.0000	0.0000	0.0000	0.0000	0.0000	
373	0.9910	-8.05	0.0000	0.0000	0.0000	0.0000	0.0000	
374	0.9580	-8.36	0.0000	0.0000	0.0000	0.0000	0.0000	
376	0.9430	-8.24	0.0000	0.0000	0.0000	0.0000	0.0000	
377	1.0060	-3.30	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.48
Power flow node solution in IEEE 118-bus system (part 8)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
380	1.0400	-1.08	0.0000	0.0000	0.0000	0.0000	0.0000	
385	0.9850	2.49	0.0000	0.0000	0.0000	0.0000	0.0000	
387	1.0150	1.38	0.0000	0.0000	0.0000	0.0000	0.0000	
389	1.0050	9.67	0.0000	0.0000	0.0000	0.0000	0.0000	
390	0.9850	3.27	0.0000	0.0000	0.0000	0.0000	0.0000	
391	0.9800	3.28	0.0000	0.0000	0.0000	0.0000	0.0000	
392	0.9900	3.81	0.0000	0.0000	0.0000	0.0000	0.0000	
399	1.0100	-3.00	0.0000	0.0000	0.0000	0.0000	0.0000	
401	0.9550	-19.16	0.0000	0.0000	0.0000	0.0000	0.0000	
404	0.9980	-14.54	0.0000	0.0000	0.0000	0.0000	0.0000	
406	0.9900	-16.84	0.0000	0.0000	0.0000	0.0000	0.0000	
408	1.0150	-8.88	0.0000	0.0000	0.0000	0.0000	0.0000	
410	1.0500	5.86	0.0000	0.0000	0.0000	0.0000	0.0000	
412	0.9900	-17.66	0.0000	0.0000	0.0000	0.0000	0.0000	
415	0.9700	-18.79	0.0000	0.0000	0.0000	0.0000	0.0000	
418	0.9730	-18.49	0.0000	0.0000	0.0000	0.0000	0.0000	
419	0.9620	-18.96	0.0000	0.0000	0.0000	0.0000	0.0000	
424	0.9920	-9.03	0.0000	0.0000	0.0000	0.0000	0.0000	
425	1.0500	-2.01	0.0000	0.0000	0.0000	0.0000	0.0000	
426	1.0150	-0.07	0.0000	0.0000	0.0000	0.0000	0.0000	
427	0.9680	-14.58	0.0000	0.0000	0.0000	0.0000	0.0000	
431	0.9670	-17.21	0.0000	0.0000	0.0000	0.0000	0.0000	
432	0.9630	-15.13	0.0000	0.0000	0.0000	0.0000	0.0000	
434	0.9840	-18.93	0.0000	0.0000	0.0000	0.0000	0.0000	
436	0.9800	-19.39	0.0000	0.0000	0.0000	0.0000	0.0000	
440	0.9700	-22.88	0.0000	0.0000	0.0000	0.0000	0.0000	
442	0.9850	-21.65	0.0000	0.0000	0.0000	0.0000	0.0000	
446	1.0050	-11.65	0.0000	0.0000	0.0000	0.0000	0.0000	
449	1.0250	-9.21	0.0000	0.0000	0.0000	0.0000	0.0000	
454	0.9550	-14.93	0.0000	0.0000	0.0000	0.0000	0.0000	
455	0.9520	-15.22	0.0000	0.0000	0.0000	0.0000	0.0000	
456	0.9540	-15.03	0.0000	0.0000	0.0000	0.0000	0.0000	
459	0.9850	-10.88	0.0000	0.0000	0.0000	0.0000	0.0000	
461	0.9950	-6.10	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.49
Power flow node solution in IEEE 118-bus system (part 9)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
462	0.9980	-6.72	0.0000	0.0000	0.0000	0.0000	0.0000	
465	1.0050	-2.48	0.0000	0.0000	0.0000	0.0000	0.0000	
466	1.0500	-2.67	0.0000	0.0000	0.0000	0.0000	0.0000	
469	1.0350	0.00	0.0000	0.0000	0.0000	0.0000	0.0000	
470	0.9840	-7.42	0.0000	0.0000	0.0000	0.0000	0.0000	
472	0.9800	-8.99	0.0000	0.0000	0.0000	0.0000	0.0000	
473	0.9910	-8.05	0.0000	0.0000	0.0000	0.0000	0.0000	
474	0.9580	-8.36	0.0000	0.0000	0.0000	0.0000	0.0000	
476	0.9430	-8.24	0.0000	0.0000	0.0000	0.0000	0.0000	
477	1.0060	-3.30	0.0000	0.0000	0.0000	0.0000	0.0000	
480	1.0400	-1.08	0.0000	0.0000	0.0000	0.0000	0.0000	
485	0.9850	2.49	0.0000	0.0000	0.0000	0.0000	0.0000	
487	1.0150	1.38	0.0000	0.0000	0.0000	0.0000	0.0000	
489	1.0050	9.67	0.0000	0.0000	0.0000	0.0000	0.0000	
490	0.9850	3.27	0.0000	0.0000	0.0000	0.0000	0.0000	
491	0.9800	3.28	0.0000	0.0000	0.0000	0.0000	0.0000	
492	0.9900	3.81	0.0000	0.0000	0.0000	0.0000	0.0000	
499	1.0100	-3.00	0.0000	0.0000	0.0000	0.0000	0.0000	
501	0.9550	-19.16	0.0000	-0.0304	0.0000	0.0000	0.0000	Riverside2
504	0.9980	-14.54	0.0000	-0.1279	0.0000	0.0000	0.0000	NCarlisle2
506	0.9900	-16.84	0.0000	0.1627	0.0000	0.0000	0.0000	Kankakee2
508	1.0150	-8.88	0.0000	0.5671	0.0000	0.0000	0.0000	Olive2
510	1.0500	5.86	4.5000	-0.5127	0.0000	0.0000	0.0000	Breed2
512	0.9900	-17.66	0.8500	0.9166	0.0000	0.0000	0.0000	TwnBranch2
515	0.9700	-18.79	0.0000	0.0797	0.0000	0.0000	0.0000	FortWayne2
518	0.9730	-18.49	0.0000	0.2901	0.0000	0.0000	0.0000	McKinley2
519	0.9620	-18.96	0.0000	-0.1431	0.0000	0.0000	0.0000	Lincoln2
524	0.9920	-9.03	0.0000	-0.1498	0.0000	0.0000	0.0000	Trenton2
525	1.0500	-2.01	2.2000	0.5220	0.0000	0.0000	0.0000	TannersCk2
526	1.0150	-0.07	3.1400	0.0672	0.0000	0.0000	0.0000	TannersCk4
527	0.9680	-14.58	0.0000	0.0363	0.0000	0.0000	0.0000	Madison2
531	0.9670	-17.21	0.0700	0.3274	0.0000	0.0000	0.0000	DeerCreek2
532	0.9630	-15.13	0.0000	-0.1637	0.0000	0.0000	0.0000	Delaware2
534	0.9840	-18.93	0.0000	-0.1639	0.0000	0.0000	0.0000	Rockhill2
536	0.9800	-19.39	0.0000	0.0842	0.0000	0.0000	0.0000	Sterling2
540	0.9700	-22.88	0.0000	0.2876	0.0000	0.0000	0.0000	West End2

Table B.50
Power flow node solution in IEEE 118-bus system (part 10)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
542	0.9850	-21.65	0.0000	0.4094	0.0000	0.0000	0.0000	Howard2
546	1.0050	-11.65	0.1900	-0.0491	0.0000	0.0000	0.0000	W.Lancstr2
549	1.0250	-9.21	2.0400	1.1711	0.0000	0.0000	0.0000	Philo2
554	0.9550	-14.93	0.4800	0.0365	0.0000	0.0000	0.0000	Torrey2
555	0.9520	-15.22	0.0000	0.0461	0.0000	0.0000	0.0000	Wagenhals2
556	0.9540	-15.03	0.0000	-0.0244	0.0000	0.0000	0.0000	Sunnyside2
559	0.9850	-10.88	1.5500	0.8034	0.0000	0.0000	0.0000	Tidd2
561	0.9950	-6.10	1.6000	-0.4196	0.0000	0.0000	0.0000	W. Kammer2
562	0.9980	-6.72	0.0000	0.0119	0.0000	0.0000	0.0000	Natrium2
565	1.0050	-2.48	3.9100	0.6395	0.0000	0.0000	0.0000	Muskingum2
566	1.0500	-2.67	3.9200	0.0700	0.0000	0.0000	0.0000	Muskingum2
569	1.0350	0.00	5.1408	-0.7068	0.0000	0.0000	0.0000	Sporn2
570	0.9840	-7.42	0.0000	0.0970	0.0000	0.0000	0.0000	Portsmoth2
572	0.9800	-8.99	0.0000	-0.1114	0.0000	0.0000	0.0000	Hillsboro2
573	0.9910	-8.05	0.0000	0.0966	0.0000	0.0000	0.0000	Sargents2
574	0.9580	-8.36	0.0000	-0.0574	0.0000	0.0000	0.0000	Bellefont2
576	0.9430	-8.24	0.0000	0.0516	0.0000	0.0000	0.0000	Darrah2
577	1.0060	-3.30	0.0000	0.1206	0.0000	0.0000	0.0000	Turner2
580	1.0400	-1.08	4.7700	1.1096	0.0000	0.0000	0.0000	Cabin Crk2
585	0.9850	2.49	0.0000	-0.0568	0.0000	0.0000	0.0000	BeaverCrk2
587	1.0150	1.38	0.0400	0.1103	0.0000	0.0000	0.0000	Pineville2
589	1.0050	9.67	6.0700	-0.0573	0.0000	0.0000	0.0000	ClinchRvr2
590	0.9850	3.27	0.0000	0.5916	0.0000	0.0000	0.0000	Holston2
591	0.9800	3.28	0.0000	-0.1310	0.0000	0.0000	0.0000	HolstonTP2
592	0.9900	3.81	0.0000	-0.1403	0.0000	0.0000	0.0000	Saltville2
599	1.0100	-3.00	0.0000	-0.1758	0.0000	0.0000	0.0000	Hinton2
600	1.0170	-2.01	0.0000	0.0000	0.0000	0.0000	0.0000	
603	1.0100	-5.74	0.0000	0.0000	0.0000	0.0000	0.0000	
604	0.9710	-8.31	0.0000	0.0000	0.0000	0.0000	0.0000	
605	0.9650	-9.41	0.0000	0.0000	0.0000	0.0000	0.0000	
607	0.9520	-12.47	0.0000	0.0000	0.0000	0.0000	0.0000	
610	0.9730	-11.91	0.0000	0.0000	0.0000	0.0000	0.0000	
611	0.9800	-10.26	0.0000	0.0000	0.0000	0.0000	0.0000	
612	0.9750	-15.01	0.0000	0.0000	0.0000	0.0000	0.0000	
613	0.9930	-16.26	0.0000	0.0000	0.0000	0.0000	0.0000	
616	1.0050	-3.07	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.51
Power flow node solution in IEEE 118-bus system (part 11)

Node	| V |	∠ V	PG	QG	PL	QL	QC	Name
700	1.0170	-2.01	0.0000	0.0000	0.0000	0.0000	0.0000	
703	1.0100	-5.74	0.0000	0.0000	0.0000	0.0000	0.0000	
704	0.9710	-8.31	0.0000	0.0000	0.0000	0.0000	0.0000	
705	0.9650	-9.41	0.0000	0.0000	0.0000	0.0000	0.0000	
707	0.9520	-12.47	0.0000	0.0000	0.0000	0.0000	0.0000	
710	0.9730	-11.91	0.0000	0.0000	0.0000	0.0000	0.0000	
711	0.9800	-10.26	0.0000	0.0000	0.0000	0.0000	0.0000	
712	0.9750	-15.01	0.0000	0.0000	0.0000	0.0000	0.0000	
713	0.9930	-16.26	0.0000	0.0000	0.0000	0.0000	0.0000	
716	1.0050	-3.07	0.0000	0.0000	0.0000	0.0000	0.0000	
800	1.0170	-2.01	0.0000	0.0000	0.0000	0.0000	0.0000	
803	1.0100	-5.74	0.0000	0.0000	0.0000	0.0000	0.0000	
804	0.9710	-8.31	0.0000	0.0000	0.0000	0.0000	0.0000	
805	0.9650	-9.41	0.0000	0.0000	0.0000	0.0000	0.0000	
807	0.9520	-12.47	0.0000	0.0000	0.0000	0.0000	0.0000	
810	0.9730	-11.91	0.0000	0.0000	0.0000	0.0000	0.0000	
811	0.9800	-10.26	0.0000	0.0000	0.0000	0.0000	0.0000	
812	0.9750	-15.01	0.0000	0.0000	0.0000	0.0000	0.0000	
813	0.9930	-16.26	0.0000	0.0000	0.0000	0.0000	0.0000	
816	1.0050	-3.07	0.0000	0.0000	0.0000	0.0000	0.0000	
900	1.0170	-2.01	2.5200	0.9569	0.0000	0.0000	0.0000	Glen Lyn2
903	1.0100	-5.74	0.4000	0.7550	0.0000	0.0000	0.0000	Claytor2
904	0.9710	-8.31	0.0000	0.0228	0.0000	0.0000	0.0000	Hancock2
905	0.9650	-9.41	0.0000	-0.1842	0.0000	0.0000	0.0000	Roanoke2
907	0.9520	-12.47	0.0000	0.0650	0.0000	0.0000	0.0000	Reusens2
910	0.9730	-11.91	0.0000	0.0024	0.0000	0.0000	0.0000	Fieldale2
911	0.9800	-10.26	0.3600	-0.0184	0.0000	0.0000	0.0000	Dan River2
912	0.9750	-15.01	0.0000	0.4149	0.0000	0.0000	0.0000	Danville2
913	0.9930	-16.26	0.0000	0.0774	0.0000	0.0000	0.0000	DeerCk TP2
916	1.0050	-3.07	0.0000	0.3758	0.0000	0.0000	0.0000	Kyger Crk2
Total			43.7508	7.9523	42.4200	14.3800	0.8440	

Table B.52
Power flow branch solution in IEEE 118-bus system (Part 1)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
1	2	-0.1223	-0.1309	-0.1233	-0.1105	0.0010	-0.0204
1	3	-0.3877	-0.1696	-0.3902	-0.1678	0.0025	-0.0018
4	5	-1.0382	-0.2449	-1.0402	-0.2519	0.0020	0.0070
3	5	-0.6839	-0.1430	-0.6964	-0.1713	0.0125	0.0283
5	6	0.8900	0.0370	0.8806	0.0084	0.0094	0.0286
6	7	0.3606	-0.0489	0.3600	-0.0463	0.0006	-0.0026
8	9	-4.4068	-0.9103	-4.4528	-0.2505	0.0460	-0.6598
9	10	-4.4528	-0.2505	-4.5000	0.5127	0.0472	-0.7632
4	11	0.6482	-0.0030	0.6394	-0.0148	0.0088	0.0118
5	11	0.7786	0.0263	0.7663	0.0022	0.0123	0.0241
11	12	0.3487	-0.3551	0.3472	-0.3552	0.0015	0.0001
2	12	-0.3233	-0.2005	-0.3261	-0.1946	0.0028	-0.0059
3	12	-0.0963	-0.1248	-0.0974	-0.0894	0.0011	-0.0354
7	12	0.1700	-0.0663	0.1697	-0.0589	0.0003	-0.0074
11	13	0.3570	0.1124	0.3537	0.1196	0.0033	-0.0072
12	14	0.1901	0.0244	0.1893	0.0394	0.0008	-0.0150
13	15	0.0137	-0.0404	0.0137	0.0184	0.0000	-0.0589
14	15	0.0493	0.0294	0.0490	0.0763	0.0003	-0.0469
12	16	0.0818	0.0422	0.0816	0.0623	0.0002	-0.0200
15	17	-1.0404	-0.2358	-1.0562	-0.2453	0.0158	0.0095
16	17	-0.1684	-0.0377	-0.1697	0.0026	0.0013	-0.0403
17	18	0.8053	0.2414	0.7965	0.2177	0.0088	0.0237
18	19	0.1965	0.1678	0.1957	0.1749	0.0008	-0.0071
19	20	-0.1097	0.0529	-0.1102	0.0782	0.0005	-0.0254
15	19	0.1193	0.1560	0.1188	0.1637	0.0005	-0.0077
20	21	-0.2902	0.0482	-0.2919	0.0599	0.0018	-0.0117
21	22	-0.4319	-0.0201	-0.4362	-0.0170	0.0043	-0.0031
22	23	-0.5362	-0.0670	-0.5467	-0.0769	0.0105	0.0099
23	24	0.0733	0.1062	0.0730	0.1544	0.0003	-0.0483
23	25	-1.6241	-0.2637	-1.6660	-0.3878	0.0419	0.1241
25	27	1.4407	0.3036	1.3767	0.1548	0.0640	0.1488
27	28	0.3309	-0.0063	0.3286	0.0038	0.0022	-0.0101
28	29	0.1586	-0.0662	0.1579	-0.0470	0.0007	-0.0192
8	30	0.7217	0.2499	0.7183	0.7279	0.0034	-0.4780
26	30	2.2333	-0.1341	2.1942	0.3616	0.0391	-0.4958
17	31	0.1428	0.1149	0.1409	0.1473	0.0018	-0.0323

Table B.53
Power flow branch solution in IEEE 118-bus system (Part 2)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
29	31	-0.0821	-0.0870	-0.0822	-0.0798	0.0002	-0.0072
23	32	0.9340	0.0507	0.9061	0.0619	0.0280	-0.0112
31	32	-0.3013	0.1249	-0.3048	0.1367	0.0035	-0.0119
27	32	0.1275	0.0170	0.1270	0.0336	0.0004	-0.0166
15	33	0.0837	-0.0458	0.0834	-0.0168	0.0003	-0.0290
19	34	-0.0258	-0.1073	-0.0264	-0.0492	0.0006	-0.0581
35	36	0.0070	0.0338	0.0070	0.0364	0.0000	-0.0026
35	37	-0.3370	-0.1238	-0.3385	-0.1176	0.0015	-0.0062
33	37	-0.1466	-0.1068	-0.1479	-0.0760	0.0013	-0.0308
34	36	0.3039	0.0465	0.3030	0.0494	0.0009	-0.0029
34	37	-0.9285	-0.4022	-0.9312	-0.4025	0.0027	0.0003
37	39	0.5422	0.0289	0.5326	0.0228	0.0097	0.0060
37	40	0.4338	-0.0372	0.4224	-0.0291	0.0114	-0.0081
30	38	0.6125	0.1650	0.6100	0.5394	0.0025	-0.3743
39	40	0.2626	-0.0872	0.2611	-0.0774	0.0015	-0.0098
40	41	0.1482	0.0138	0.1479	0.0241	0.0003	-0.0103
40	42	-0.1247	-0.0626	-0.1257	-0.0214	0.0010	-0.0412
41	42	-0.2221	-0.0759	-0.2244	-0.0508	0.0023	-0.0251
43	44	-0.1718	-0.0116	-0.1737	0.0392	0.0019	-0.0508
34	43	0.0082	0.0181	0.0082	0.0584	0.0001	-0.0404
44	45	-0.3337	0.0561	-0.3364	0.0671	0.0027	-0.0110
45	46	-0.3669	-0.0351	-0.3724	-0.0209	0.0055	-0.0141
46	47	-0.3150	-0.0105	-0.3188	0.0093	0.0037	-0.0198
46	48	-0.1474	-0.0586	-0.1487	-0.0144	0.0014	-0.0442
47	49	-0.0860	-0.1123	-0.0863	-0.0966	0.0003	-0.0156
42	49	-0.6551	0.0536	-0.6871	-0.0045	0.0320	0.0582
42	49	-0.6551	0.0536	-0.6871	-0.0045	0.0320	0.0582
45	49	-0.4995	-0.0205	-0.5170	-0.0233	0.0175	0.0027
48	49	-0.3487	0.0319	-0.3509	0.0390	0.0021	-0.0072
49	50	0.5388	0.1339	0.5309	0.1309	0.0079	0.0030
49	51	0.6690	0.2042	0.6460	0.1734	0.0230	0.0308
51	52	0.2864	0.0623	0.2845	0.0698	0.0019	-0.0075
52	53	0.1045	0.0198	0.1040	0.0543	0.0006	-0.0345
53	54	-0.1260	-0.0557	-0.1265	-0.0301	0.0005	-0.0256
49	54	0.3810	0.1313	0.3690	0.1561	0.0120	-0.0248
49	54	0.3807	0.1124	0.3669	0.1379	0.0138	-0.0255

Table B.54
Power flow branch solution in IEEE 118-bus system (Part 3)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
54	55	0.0716	0.0144	0.0715	0.0323	0.0001	-0.0179
54	56	0.1885	0.0425	0.1884	0.0488	0.0001	-0.0063
55	56	-0.2162	-0.0576	-0.2165	-0.0550	0.0003	-0.0026
56	57	-0.2319	-0.0903	-0.2342	-0.0743	0.0023	-0.0160
50	57	0.3609	0.0909	0.3542	0.1043	0.0067	-0.0133
56	58	-0.0684	-0.0363	-0.0686	-0.0148	0.0002	-0.0216
51	58	0.1896	0.0311	0.1886	0.0448	0.0010	-0.0137
54	59	-0.3008	-0.0764	-0.3059	-0.0434	0.0051	-0.0330
56	59	-0.2772	-0.0433	-0.2842	-0.0109	0.0070	-0.0323
56	59	-0.2906	-0.0407	-0.2980	-0.0124	0.0075	-0.0282
55	59	-0.3422	-0.0840	-0.3485	-0.0596	0.0063	-0.0244
59	60	-0.4444	0.0389	-0.4510	0.0457	0.0066	-0.0068
59	61	-0.5290	0.0537	-0.5386	0.0477	0.0096	0.0060
60	61	-1.1306	0.0867	-1.1341	0.0834	0.0034	0.0032
60	62	-0.1003	-0.0710	-0.1005	-0.0572	0.0002	-0.0137
61	62	0.2562	-0.1388	0.2555	-0.1323	0.0007	-0.0066
63	64	-1.4833	-0.6534	-1.4879	-0.5004	0.0046	-0.1530
38	65	-1.7836	-0.5746	-1.8142	0.1167	0.0307	-0.6912
64	65	-1.8168	-0.6536	-1.8266	-0.3869	0.0098	-0.2667
49	66	-1.3243	0.0437	-1.3544	-0.0833	0.0301	0.1269
49	66	-1.3243	0.0437	-1.3544	-0.0833	0.0301	0.1269
62	66	-0.3721	-0.1732	-0.3798	-0.1473	0.0077	-0.0259
62	67	-0.2429	-0.1443	-0.2449	-0.1217	0.0020	-0.0227
66	67	0.5315	0.1929	0.5249	0.1917	0.0066	0.0012
65	68	0.1792	-0.2623	0.1791	0.3813	0.0001	-0.6436
47	69	-0.5728	0.1216	-0.6015	0.1018	0.0287	0.0198
49	69	-0.4793	0.1121	-0.5030	0.1221	0.0237	-0.0100
69	70	1.0914	0.1614	1.0567	0.1390	0.0347	0.0224
24	70	-0.0673	-0.0296	-0.0673	0.0682	0.0000	-0.0978
70	71	0.1710	-0.1247	0.1706	-0.1178	0.0004	-0.0069
24	72	0.0103	0.0342	0.0101	0.0810	0.0002	-0.0468
71	72	0.1105	-0.0104	0.1099	0.0304	0.0006	-0.0407
71	73	0.0601	-0.1075	0.0600	-0.0966	0.0001	-0.0109
70	74	0.1611	0.1294	0.1591	0.1547	0.0020	-0.0253
70	75	-0.0027	0.0996	-0.0033	0.1319	0.0006	-0.0323
69	75	1.1060	0.2054	1.0571	0.1826	0.0488	0.0228

Table B.55
Power flow branch solution in IEEE 118-bus system (Part 4)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
74	75	-0.5209	-0.0626	-0.5245	-0.0651	0.0037	0.0026
76	77	-0.6100	-0.2115	-0.6305	-0.2448	0.0205	0.0332
69	77	0.6322	0.0661	0.6203	0.1353	0.0119	-0.0692
75	77	-0.3443	-0.0965	-0.3523	-0.0744	0.0079	-0.0221
77	78	0.4569	0.0653	0.4561	0.0754	0.0008	-0.0101
78	79	-0.2539	-0.1846	-0.2544	-0.1804	0.0005	-0.0042
77	80	-0.9597	-0.3769	-0.9772	-0.3776	0.0176	0.0007
77	80	-0.4408	-0.2066	-0.4475	-0.2068	0.0067	0.0002
79	80	-0.6444	-0.2967	-0.6520	-0.3114	0.0076	0.0148
68	81	-0.4554	-0.0984	-0.4560	0.7065	0.0006	-0.8049
77	82	-0.0290	0.1750	-0.0304	0.2523	0.0014	-0.0773
82	83	-0.4721	0.2439	-0.4754	0.2699	0.0033	-0.0260
83	84	-0.2477	0.1468	-0.2533	0.1599	0.0056	-0.0131
83	85	-0.4277	0.1200	-0.4366	0.1230	0.0089	-0.0030
84	85	-0.3633	0.0899	-0.3677	0.0924	0.0044	-0.0025
85	86	0.1717	-0.0737	0.1705	-0.0510	0.0012	-0.0226
86	87	-0.0395	-0.1510	-0.0400	-0.1103	0.0005	-0.0407
85	88	-0.5035	0.0758	-0.5089	0.0751	0.0054	0.0006
85	89	-0.7126	0.0065	-0.7251	-0.0375	0.0125	0.0440
88	89	-0.9889	-0.0249	-1.0028	-0.0771	0.0139	0.0522
89	90	0.5823	-0.0469	0.5649	-0.0577	0.0174	0.0108
89	90	1.1085	-0.0538	1.0797	-0.0698	0.0289	0.0161
90	91	0.0146	0.0441	0.0145	0.0645	0.0001	-0.0204
89	92	2.0150	-0.0207	1.9753	-0.1691	0.0398	0.1484
89	92	0.6362	-0.0505	0.6205	-0.0727	0.0158	0.0222
91	92	-0.0855	-0.0665	-0.0859	-0.0361	0.0004	-0.0304
92	93	0.5760	-0.1166	0.5670	-0.1250	0.0090	0.0084
92	94	0.5219	-0.1522	0.5077	-0.1591	0.0142	0.0069
93	94	0.4470	-0.1950	0.4416	-0.1944	0.0054	-0.0006
94	95	0.4086	0.0901	0.4062	0.0931	0.0024	-0.0030
80	96	0.1892	0.2110	0.1862	0.2466	0.0030	-0.0356
82	96	-0.0983	-0.0661	-0.0985	-0.0134	0.0002	-0.0528
94	96	0.1979	-0.0983	0.1966	-0.0798	0.0013	-0.0185
80	97	0.2636	0.2576	0.2612	0.2720	0.0024	-0.0144
80	98	0.2890	0.0833	0.2870	0.1045	0.0021	-0.0211
80	99	0.1954	0.0820	0.1933	0.1299	0.0021	-0.0478

Table B.56
Power flow branch solution in IEEE 118-bus system (Part 5)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
92	100	0.3155	-0.1655	0.3076	-0.1539	0.0079	-0.0116
94	100	0.0428	-0.5053	0.0387	-0.4579	0.0041	-0.0473
95	96	-0.0138	-0.2169	-0.0146	-0.2051	0.0008	-0.0118
96	97	-0.1103	-0.2017	-0.1112	-0.1820	0.0008	-0.0198
98	100	-0.0530	0.0244	-0.0532	0.0731	0.0002	-0.0487
99	100	-0.2267	-0.0459	-0.2276	-0.0279	0.0009	-0.0180
100	101	-0.1673	0.2290	-0.1697	0.2513	0.0024	-0.0223
92	102	0.4464	-0.0839	0.4438	-0.0813	0.0026	-0.0026
101	102	-0.3897	0.1013	-0.3938	0.1113	0.0041	-0.0100
100	103	1.2168	-0.2211	1.1933	-0.2430	0.0235	0.0220
100	104	0.5619	0.1070	0.5474	0.0948	0.0145	0.0122
103	104	0.3241	0.1391	0.3182	0.1588	0.0060	-0.0197
103	105	0.4332	0.1290	0.4222	0.1354	0.0110	-0.0064
100	106	0.6040	0.0954	0.5818	0.0720	0.0222	0.0234
104	105	0.4856	0.0264	0.4831	0.0262	0.0025	0.0003
105	106	0.0882	0.0384	0.0881	0.0511	0.0001	-0.0127
105	107	0.2675	-0.0236	0.2634	0.0058	0.0041	-0.0294
105	108	0.2396	-0.1113	0.2377	-0.0992	0.0019	-0.0121
106	107	0.2399	-0.0370	0.2366	-0.0052	0.0033	-0.0318
108	109	0.2177	-0.1092	0.2170	-0.1039	0.0007	-0.0053
103	110	0.6060	0.0839	0.5915	0.0620	0.0145	0.0219
109	110	0.1370	-0.1339	0.1360	-0.1177	0.0010	-0.0162
110	111	-0.3570	0.0095	-0.3600	0.0184	0.0030	-0.0089
110	112	0.6946	-0.3060	0.6800	-0.2849	0.0146	-0.0211
17	113	0.0160	0.0508	0.0160	0.0582	0.0000	-0.0075
32	113	0.0458	-0.1795	0.0440	-0.1356	0.0017	-0.0439
32	114	0.0925	0.0180	0.0924	0.0325	0.0001	-0.0144
27	115	0.2084	0.0504	0.2076	0.0650	0.0008	-0.0146
114	115	0.0124	0.0025	0.0124	0.0050	0.0000	-0.0025
68	116	1.8412	-0.5269	1.8400	-0.3758	0.0012	-0.1510
12	117	0.2015	0.0520	0.2000	0.0800	0.0015	-0.0280
75	118	0.4036	0.2359	0.4002	0.2355	0.0034	0.0004
76	118	-0.0700	-0.0969	-0.0702	-0.0855	0.0002	-0.0113
120	123	-3.4052	-0.8879	-3.4052	-1.2275	0.0000	0.3396
140	141	-0.9067	-0.1694	-0.9067	-0.2013	0.0000	0.0320
132	145	-2.3001	-0.6798	-2.3001	-0.9245	0.0000	0.2447

Table B.57
Power flow branch solution in IEEE 118-bus system (Part 6)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
152	153	-2.3936	-0.8329	-2.3936	-1.1139	0.0000	0.2810
174	178	-1.4833	-0.5456	-1.4833	-0.6534	0.0000	0.1078
176	179	-0.3289	-0.1496	-0.3289	-0.1532	0.0000	0.0036
181	180	-0.0900	-0.6168	-0.0900	-0.6317	0.0000	0.0149
184	183	1.2067	-0.9159	1.2067	-1.0065	0.0000	0.0907
195	196	0.4560	-0.6802	0.4560	-0.7065	0.0000	0.0262
5	120	-3.4052	-0.8879	-3.4052	-0.8879	0.0000	0.0000
25	140	-0.9067	-0.1694	-0.9067	-0.1694	0.0000	0.0000
17	132	-2.3001	-0.6798	-2.3001	-0.6798	0.0000	0.0000
37	152	-2.3936	-0.8329	-2.3936	-0.8329	0.0000	0.0000
59	174	-1.4833	-0.5456	-1.4833	-0.5456	0.0000	0.0000
61	176	-0.3289	-0.1496	-0.3289	-0.1496	0.0000	0.0000
66	181	-0.0900	-0.6168	-0.0900	-0.6168	0.0000	0.0000
69	184	1.2067	-0.9159	1.2067	-0.9159	0.0000	0.0000
80	195	0.4560	-0.6802	0.4560	-0.6802	0.0000	0.0000
123	8	-3.4052	-1.2275	-3.4052	-1.2275	0.0000	0.0000
141	26	-0.9067	-0.2013	-0.9067	-0.2013	0.0000	0.0000
145	30	-2.3001	-0.9245	-2.3001	-0.9245	0.0000	0.0000
153	38	-2.3936	-1.1139	-2.3936	-1.1139	0.0000	0.0000
178	63	-1.4833	-0.6534	-1.4833	-0.6534	0.0000	0.0000
179	64	-0.3289	-0.1532	-0.3289	-0.1532	0.0000	0.0000
180	65	-0.0900	-0.6317	-0.0900	-0.6317	0.0000	0.0000
183	68	1.2067	-1.0065	1.2067	-1.0065	0.0000	0.0000
196	81	0.4560	-0.7065	0.4560	-0.7065	0.0000	0.0000
1	201	0.0000	0.0304	0.0000	0.0304	0.0000	0.0000
201	301	0.0000	0.0304	0.0000	0.0304	0.0000	0.0000
301	401	0.0000	0.0304	0.0000	0.0304	0.0000	0.0000
401	501	0.0000	0.0304	0.0000	0.0304	0.0000	0.0000
4	204	0.0000	0.1279	0.0000	0.1279	0.0000	0.0000
204	304	0.0000	0.1279	0.0000	0.1279	0.0000	0.0000
304	404	0.0000	0.1279	0.0000	0.1279	0.0000	0.0000
404	504	0.0000	0.1279	0.0000	0.1279	0.0000	0.0000
6	206	0.0000	-0.1627	0.0000	-0.1627	0.0000	0.0000
206	306	0.0000	-0.1627	0.0000	-0.1627	0.0000	0.0000
306	406	0.0000	-0.1627	0.0000	-0.1627	0.0000	0.0000
406	506	0.0000	-0.1627	0.0000	-0.1627	0.0000	0.0000

Table B.58
Power flow branch solution in IEEE 118-bus system (Part 7)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
8	208	0.0000	-0.5671	0.0000	-0.5671	0.0000	0.0000
208	308	0.0000	-0.5671	0.0000	-0.5671	0.0000	0.0000
308	408	0.0000	-0.5671	0.0000	-0.5671	0.0000	0.0000
408	508	0.0000	-0.5671	0.0000	-0.5671	0.0000	0.0000
10	210	-4.5000	0.5127	-4.5000	0.5127	0.0000	0.0000
210	310	-4.5000	0.5127	-4.5000	0.5127	0.0000	0.0000
310	410	-4.5000	0.5127	-4.5000	0.5127	0.0000	0.0000
410	510	-4.5000	0.5127	-4.5000	0.5127	0.0000	0.0000
12	212	-0.8500	-0.9166	-0.8500	-0.9166	0.0000	0.0000
212	312	-0.8500	-0.9166	-0.8500	-0.9166	0.0000	0.0000
312	412	-0.8500	-0.9166	-0.8500	-0.9166	0.0000	0.0000
412	512	-0.8500	-0.9166	-0.8500	-0.9166	0.0000	0.0000
15	215	0.0000	-0.0797	0.0000	-0.0797	0.0000	0.0000
215	315	0.0000	-0.0797	0.0000	-0.0797	0.0000	0.0000
315	415	0.0000	-0.0797	0.0000	-0.0797	0.0000	0.0000
415	515	0.0000	-0.0797	0.0000	-0.0797	0.0000	0.0000
18	218	0.0000	-0.2901	0.0000	-0.2901	0.0000	0.0000
218	318	0.0000	-0.2901	0.0000	-0.2901	0.0000	0.0000
318	418	0.0000	-0.2901	0.0000	-0.2901	0.0000	0.0000
418	518	0.0000	-0.2901	0.0000	-0.2901	0.0000	0.0000
19	219	0.0000	0.1431	0.0000	0.1431	0.0000	0.0000
219	319	0.0000	0.1431	0.0000	0.1431	0.0000	0.0000
319	419	0.0000	0.1431	0.0000	0.1431	0.0000	0.0000
419	519	0.0000	0.1431	0.0000	0.1431	0.0000	0.0000
24	224	0.0000	0.1498	0.0000	0.1498	0.0000	0.0000
224	324	0.0000	0.1498	0.0000	0.1498	0.0000	0.0000
324	424	0.0000	0.1498	0.0000	0.1498	0.0000	0.0000
424	524	0.0000	0.1498	0.0000	0.1498	0.0000	0.0000
25	225	-2.2000	-0.5220	-2.2000	-0.5220	0.0000	0.0000
225	325	-2.2000	-0.5220	-2.2000	-0.5220	0.0000	0.0000
325	425	-2.2000	-0.5220	-2.2000	-0.5220	0.0000	0.0000
425	525	-2.2000	-0.5220	-2.2000	-0.5220	0.0000	0.0000
26	226	-3.1400	-0.0672	-3.1400	-0.0672	0.0000	0.0000
226	326	-3.1400	-0.0672	-3.1400	-0.0672	0.0000	0.0000
326	426	-3.1400	-0.0672	-3.1400	-0.0672	0.0000	0.0000
426	526	-3.1400	-0.0672	-3.1400	-0.0672	0.0000	0.0000

Table B.59
Power flow branch solution in IEEE 118-bus system (Part 8)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
27	227	0.0000	-0.0363	0.0000	-0.0363	0.0000	0.0000
227	327	0.0000	-0.0363	0.0000	-0.0363	0.0000	0.0000
327	427	0.0000	-0.0363	0.0000	-0.0363	0.0000	0.0000
427	527	0.0000	-0.0363	0.0000	-0.0363	0.0000	0.0000
31	231	-0.0700	-0.3274	-0.0700	-0.3274	0.0000	0.0000
231	331	-0.0700	-0.3274	-0.0700	-0.3274	0.0000	0.0000
331	431	-0.0700	-0.3274	-0.0700	-0.3274	0.0000	0.0000
431	531	-0.0700	-0.3274	-0.0700	-0.3274	0.0000	0.0000
32	232	0.0000	0.1637	0.0000	0.1637	0.0000	0.0000
232	332	0.0000	0.1637	0.0000	0.1637	0.0000	0.0000
332	432	0.0000	0.1637	0.0000	0.1637	0.0000	0.0000
432	532	0.0000	0.1637	0.0000	0.1637	0.0000	0.0000
34	234	0.0000	0.1639	0.0000	0.1639	0.0000	0.0000
234	334	0.0000	0.1639	0.0000	0.1639	0.0000	0.0000
334	434	0.0000	0.1639	0.0000	0.1639	0.0000	0.0000
434	534	0.0000	0.1639	0.0000	0.1639	0.0000	0.0000
36	236	0.0000	-0.0842	0.0000	-0.0842	0.0000	0.0000
236	336	0.0000	-0.0842	0.0000	-0.0842	0.0000	0.0000
336	436	0.0000	-0.0842	0.0000	-0.0842	0.0000	0.0000
436	536	0.0000	-0.0842	0.0000	-0.0842	0.0000	0.0000
40	240	0.0000	-0.2876	0.0000	-0.2876	0.0000	0.0000
240	340	0.0000	-0.2876	0.0000	-0.2876	0.0000	0.0000
340	440	0.0000	-0.2876	0.0000	-0.2876	0.0000	0.0000
440	540	0.0000	-0.2876	0.0000	-0.2876	0.0000	0.0000
42	242	0.0000	-0.4094	0.0000	-0.4094	0.0000	0.0000
242	342	0.0000	-0.4094	0.0000	-0.4094	0.0000	0.0000
342	442	0.0000	-0.4094	0.0000	-0.4094	0.0000	0.0000
442	542	0.0000	-0.4094	0.0000	-0.4094	0.0000	0.0000
46	246	-0.1900	0.0491	-0.1900	0.0491	0.0000	0.0000
246	346	-0.1900	0.0491	-0.1900	0.0491	0.0000	0.0000
346	446	-0.1900	0.0491	-0.1900	0.0491	0.0000	0.0000
446	546	-0.1900	0.0491	-0.1900	0.0491	0.0000	0.0000
49	249	-2.0400	-1.1711	-2.0400	-1.1711	0.0000	0.0000
249	349	-2.0400	-1.1711	-2.0400	-1.1711	0.0000	0.0000
349	449	-2.0400	-1.1711	-2.0400	-1.1711	0.0000	0.0000
449	549	-2.0400	-1.1711	-2.0400	-1.1711	0.0000	0.0000

Table B.60
Power flow branch solution in IEEE 118-bus system (Part 9)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
54	254	-0.4800	-0.0365	-0.4800	-0.0365	0.0000	0.0000
254	354	-0.4800	-0.0365	-0.4800	-0.0365	0.0000	0.0000
354	454	-0.4800	-0.0365	-0.4800	-0.0365	0.0000	0.0000
454	554	-0.4800	-0.0365	-0.4800	-0.0365	0.0000	0.0000
55	255	0.0000	-0.0461	0.0000	-0.0461	0.0000	0.0000
255	355	0.0000	-0.0461	0.0000	-0.0461	0.0000	0.0000
355	455	0.0000	-0.0461	0.0000	-0.0461	0.0000	0.0000
455	555	0.0000	-0.0461	0.0000	-0.0461	0.0000	0.0000
56	256	0.0000	0.0244	0.0000	0.0244	0.0000	0.0000
256	356	0.0000	0.0244	0.0000	0.0244	0.0000	0.0000
356	456	0.0000	0.0244	0.0000	0.0244	0.0000	0.0000
456	556	0.0000	0.0244	0.0000	0.0244	0.0000	0.0000
59	259	-1.5500	-0.8034	-1.5500	-0.8034	0.0000	0.0000
259	359	-1.5500	-0.8034	-1.5500	-0.8034	0.0000	0.0000
359	459	-1.5500	-0.8034	-1.5500	-0.8034	0.0000	0.0000
459	559	-1.5500	-0.8034	-1.5500	-0.8034	0.0000	0.0000
61	261	-1.6000	0.4196	-1.6000	0.4196	0.0000	0.0000
261	361	-1.6000	0.4196	-1.6000	0.4196	0.0000	0.0000
361	461	-1.6000	0.4196	-1.6000	0.4196	0.0000	0.0000
461	561	-1.6000	0.4196	-1.6000	0.4196	0.0000	0.0000
62	262	0.0000	-0.0119	0.0000	-0.0119	0.0000	0.0000
262	362	0.0000	-0.0119	0.0000	-0.0119	0.0000	0.0000
362	462	0.0000	-0.0119	0.0000	-0.0119	0.0000	0.0000
462	562	0.0000	-0.0119	0.0000	-0.0119	0.0000	0.0000
65	265	-3.9100	-0.6395	-3.9100	-0.6395	0.0000	0.0000
265	365	-3.9100	-0.6395	-3.9100	-0.6395	0.0000	0.0000
365	465	-3.9100	-0.6395	-3.9100	-0.6395	0.0000	0.0000
465	565	-3.9100	-0.6395	-3.9100	-0.6395	0.0000	0.0000
66	266	-3.9200	-0.0700	-3.9200	-0.0700	0.0000	0.0000
266	366	-3.9200	-0.0700	-3.9200	-0.0700	0.0000	0.0000
366	466	-3.9200	-0.0700	-3.9200	-0.0700	0.0000	0.0000
466	566	-3.9200	-0.0700	-3.9200	-0.0700	0.0000	0.0000
69	269	-5.1408	0.7068	-5.1408	0.7068	0.0000	0.0000
269	369	-5.1408	0.7068	-5.1408	0.7068	0.0000	0.0000
369	469	-5.1408	0.7068	-5.1408	0.7068	0.0000	0.0000
469	569	-5.1408	0.7068	-5.1408	0.7068	0.0000	0.0000

Table B.61
Power flow branch solution in IEEE 118-bus system (Part 10)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
70	270	0.0000	-0.0970	0.0000	-0.0970	0.0000	0.0000
270	370	0.0000	-0.0970	0.0000	-0.0970	0.0000	0.0000
370	470	0.0000	-0.0970	0.0000	-0.0970	0.0000	0.0000
470	570	0.0000	-0.0970	0.0000	-0.0970	0.0000	0.0000
72	272	0.0000	0.1114	0.0000	0.1114	0.0000	0.0000
272	372	0.0000	0.1114	0.0000	0.1114	0.0000	0.0000
372	472	0.0000	0.1114	0.0000	0.1114	0.0000	0.0000
472	572	0.0000	0.1114	0.0000	0.1114	0.0000	0.0000
73	273	0.0000	-0.0966	0.0000	-0.0966	0.0000	0.0000
273	373	0.0000	-0.0966	0.0000	-0.0966	0.0000	0.0000
373	473	0.0000	-0.0966	0.0000	-0.0966	0.0000	0.0000
473	573	0.0000	-0.0966	0.0000	-0.0966	0.0000	0.0000
74	274	0.0000	0.0574	0.0000	0.0574	0.0000	0.0000
274	374	0.0000	0.0574	0.0000	0.0574	0.0000	0.0000
374	474	0.0000	0.0574	0.0000	0.0574	0.0000	0.0000
474	574	0.0000	0.0574	0.0000	0.0574	0.0000	0.0000
76	276	0.0000	-0.0516	0.0000	-0.0516	0.0000	0.0000
276	376	0.0000	-0.0516	0.0000	-0.0516	0.0000	0.0000
376	476	0.0000	-0.0516	0.0000	-0.0516	0.0000	0.0000
476	576	0.0000	-0.0516	0.0000	-0.0516	0.0000	0.0000
77	277	0.0000	-0.1206	0.0000	-0.1206	0.0000	0.0000
277	377	0.0000	-0.1206	0.0000	-0.1206	0.0000	0.0000
377	477	0.0000	-0.1206	0.0000	-0.1206	0.0000	0.0000
477	577	0.0000	-0.1206	0.0000	-0.1206	0.0000	0.0000
80	280	-4.7700	-1.1096	-4.7700	-1.1096	0.0000	0.0000
280	380	-4.7700	-1.1096	-4.7700	-1.1096	0.0000	0.0000
380	480	-4.7700	-1.1096	-4.7700	-1.1096	0.0000	0.0000
480	580	-4.7700	-1.1096	-4.7700	-1.1096	0.0000	0.0000
85	285	0.0000	0.0568	0.0000	0.0568	0.0000	0.0000
285	385	0.0000	0.0568	0.0000	0.0568	0.0000	0.0000
385	485	0.0000	0.0568	0.0000	0.0568	0.0000	0.0000
485	585	0.0000	0.0568	0.0000	0.0568	0.0000	0.0000
87	287	-0.0400	-0.1103	-0.0400	-0.1103	0.0000	0.0000
287	387	-0.0400	-0.1103	-0.0400	-0.1103	0.0000	0.0000
387	487	-0.0400	-0.1103	-0.0400	-0.1103	0.0000	0.0000
487	587	-0.0400	-0.1103	-0.0400	-0.1103	0.0000	0.0000

Table B.62
Power flow branch solution in IEEE 118-bus system (Part 11)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
89	289	-6.0700	0.0573	-6.0700	0.0573	0.0000	0.0000
289	389	-6.0700	0.0573	-6.0700	0.0573	0.0000	0.0000
389	489	-6.0700	0.0573	-6.0700	0.0573	0.0000	0.0000
489	589	-6.0700	0.0573	-6.0700	0.0573	0.0000	0.0000
90	290	0.0000	-0.5916	0.0000	-0.5916	0.0000	0.0000
290	390	0.0000	-0.5916	0.0000	-0.5916	0.0000	0.0000
390	490	0.0000	-0.5916	0.0000	-0.5916	0.0000	0.0000
490	590	0.0000	-0.5916	0.0000	-0.5916	0.0000	0.0000
91	291	0.0000	0.1310	0.0000	0.1310	0.0000	0.0000
291	391	0.0000	0.1310	0.0000	0.1310	0.0000	0.0000
391	491	0.0000	0.1310	0.0000	0.1310	0.0000	0.0000
491	591	0.0000	0.1310	0.0000	0.1310	0.0000	0.0000
92	292	0.0000	0.1403	0.0000	0.1403	0.0000	0.0000
292	392	0.0000	0.1403	0.0000	0.1403	0.0000	0.0000
392	492	0.0000	0.1403	0.0000	0.1403	0.0000	0.0000
492	592	0.0000	0.1403	0.0000	0.1403	0.0000	0.0000
99	299	0.0000	0.1758	0.0000	0.1758	0.0000	0.0000
299	399	0.0000	0.1758	0.0000	0.1758	0.0000	0.0000
399	499	0.0000	0.1758	0.0000	0.1758	0.0000	0.0000
499	599	0.0000	0.1758	0.0000	0.1758	0.0000	0.0000
100	600	-2.5200	-0.9569	-2.5200	-0.9569	0.0000	0.0000
600	700	-2.5200	-0.9569	-2.5200	-0.9569	0.0000	0.0000
700	800	-2.5200	-0.9569	-2.5200	-0.9569	0.0000	0.0000
800	900	-2.5200	-0.9569	-2.5200	-0.9569	0.0000	0.0000
103	603	-0.4000	-0.7550	-0.4000	-0.7550	0.0000	0.0000
603	703	-0.4000	-0.7550	-0.4000	-0.7550	0.0000	0.0000
703	803	-0.4000	-0.7550	-0.4000	-0.7550	0.0000	0.0000
803	903	-0.4000	-0.7550	-0.4000	-0.7550	0.0000	0.0000
104	604	0.0000	-0.0228	0.0000	-0.0228	0.0000	0.0000
604	704	0.0000	-0.0228	0.0000	-0.0228	0.0000	0.0000
704	804	0.0000	-0.0228	0.0000	-0.0228	0.0000	0.0000
804	904	0.0000	-0.0228	0.0000	-0.0228	0.0000	0.0000
105	605	0.0000	0.1842	0.0000	0.1842	0.0000	0.0000
605	705	0.0000	0.1842	0.0000	0.1842	0.0000	0.0000
705	805	0.0000	0.1842	0.0000	0.1842	0.0000	0.0000
805	905	0.0000	0.1842	0.0000	0.1842	0.0000	0.0000

Table B.63
Power flow branch solution in IEEE 118-bus system (Part 12)

From	To	Psend	Qsend	Prec	Qrec	Ploss	Qloss
107	607	0.0000	-0.0650	0.0000	-0.0650	0.0000	0.0000
607	707	0.0000	-0.0650	0.0000	-0.0650	0.0000	0.0000
707	807	0.0000	-0.0650	0.0000	-0.0650	0.0000	0.0000
807	907	0.0000	-0.0650	0.0000	-0.0650	0.0000	0.0000
110	610	0.0000	-0.0024	0.0000	-0.0024	0.0000	0.0000
610	710	0.0000	-0.0024	0.0000	-0.0024	0.0000	0.0000
710	810	0.0000	-0.0024	0.0000	-0.0024	0.0000	0.0000
810	910	0.0000	-0.0024	0.0000	-0.0024	0.0000	0.0000
111	611	-0.3600	0.0184	-0.3600	0.0184	0.0000	0.0000
611	711	-0.3600	0.0184	-0.3600	0.0184	0.0000	0.0000
711	811	-0.3600	0.0184	-0.3600	0.0184	0.0000	0.0000
811	911	-0.3600	0.0184	-0.3600	0.0184	0.0000	0.0000
112	612	0.0000	-0.4149	0.0000	-0.4149	0.0000	0.0000
612	712	0.0000	-0.4149	0.0000	-0.4149	0.0000	0.0000
712	812	0.0000	-0.4149	0.0000	-0.4149	0.0000	0.0000
812	912	0.0000	-0.4149	0.0000	-0.4149	0.0000	0.0000
113	613	0.0000	-0.0774	0.0000	-0.0774	0.0000	0.0000
613	713	0.0000	-0.0774	0.0000	-0.0774	0.0000	0.0000
713	813	0.0000	-0.0774	0.0000	-0.0774	0.0000	0.0000
813	913	0.0000	-0.0774	0.0000	-0.0774	0.0000	0.0000
116	616	0.0000	-0.3758	0.0000	-0.3758	0.0000	0.0000
616	716	0.0000	-0.3758	0.0000	-0.3758	0.0000	0.0000
716	816	0.0000	-0.3758	0.0000	-0.3758	0.0000	0.0000
816	916	0.0000	-0.3758	0.0000	-0.3758	0.0000	0.0000

The total P loss and Q loss are 1.3308 (p.u.) and -5.5837 (p.u.), individually.

Table B.64
System (branch) setting data (Part 1)

From	To	R	X	Y/2	Tap	Remark
1	2	0.03030	0.09990	0.01270	0.00000	
1	3	0.01290	0.04240	0.00541	0.00000	
4	5	0.00176	0.00798	0.00105	0.00000	
3	5	0.02410	0.10800	0.01420	0.00000	
5	6	0.01190	0.05400	0.00713	0.00000	
6	7	0.00459	0.02080	0.00275	0.00000	
8	9	0.00244	0.03050	0.58100	0.00000	
9	10	0.00258	0.03220	0.61500	0.00000	
4	11	0.02090	0.06880	0.00874	0.00000	
5	11	0.02030	0.06820	0.00869	0.00000	
11	12	0.00595	0.01960	0.00251	0.00000	
2	12	0.01870	0.06160	0.00786	0.00000	
3	12	0.04840	0.16000	0.02030	0.00000	
7	12	0.00862	0.03400	0.00437	0.00000	
11	13	0.02225	0.07310	0.00938	0.00000	
12	14	0.02150	0.07070	0.00908	0.00000	
13	15	0.07440	0.24440	0.03134	0.00000	
14	15	0.05950	0.19500	0.02510	0.00000	
12	16	0.02120	0.08340	0.01070	0.00000	
15	17	0.01320	0.04370	0.02220	0.00000	
16	17	0.04540	0.18010	0.02330	0.00000	
17	18	0.01230	0.05050	0.00649	0.00000	
18	19	0.01119	0.04930	0.00571	0.00000	
19	20	0.02520	0.11700	0.01490	0.00000	
15	19	0.01200	0.03940	0.00505	0.00000	
20	21	0.01830	0.08490	0.01080	0.00000	
21	22	0.02090	0.09700	0.01230	0.00000	
22	23	0.03420	0.15900	0.02020	0.00000	
23	24	0.01350	0.04920	0.02490	0.00000	
23	25	0.01560	0.08000	0.04320	0.00000	
25	27	0.03180	0.16300	0.08820	0.00000	
27	28	0.01913	0.08550	0.01080	0.00000	
28	29	0.02370	0.09430	0.01190	0.00000	
8	30	0.00431	0.05040	0.25700	0.00000	
26	30	0.00799	0.08600	0.45400	0.00000	
17	31	0.04740	0.15630	0.01995	0.00000	

Table B.65
System (branch) setting data (Part 2)

From	To	R	X	Y/2	Tap	Remark
29	31	0.01080	0.03310	0.00415	0.00000	
23	32	0.03170	0.11530	0.05865	0.00000	
31	32	0.02980	0.09850	0.01255	0.00000	
27	32	0.02290	0.07550	0.00963	0.00000	
15	33	0.03800	0.12440	0.01597	0.00000	
19	34	0.07520	0.24700	0.03160	0.00000	
35	36	0.00224	0.01020	0.00134	0.00000	
35	37	0.01100	0.04970	0.00659	0.00000	
33	37	0.04150	0.14200	0.01830	0.00000	
34	36	0.00871	0.02680	0.00284	0.00000	
34	37	0.00256	0.00940	0.00492	0.00000	
37	39	0.03210	0.10600	0.01350	0.00000	
37	40	0.05930	0.16800	0.02100	0.00000	
30	38	0.00464	0.05400	0.21100	0.00000	
39	40	0.01840	0.06050	0.00776	0.00000	
40	41	0.01450	0.04870	0.00611	0.00000	
40	42	0.05550	0.18300	0.02330	0.00000	
41	42	0.04100	0.13500	0.01720	0.00000	
43	44	0.06080	0.24540	0.03034	0.00000	
34	43	0.04130	0.16810	0.02113	0.00000	
44	45	0.02240	0.09010	0.01120	0.00000	
45	46	0.04000	0.13560	0.01660	0.00000	
46	47	0.03800	0.12700	0.01580	0.00000	
46	48	0.06010	0.18900	0.02360	0.00000	
47	49	0.01910	0.06250	0.00802	0.00000	
42	49	0.07150	0.32300	0.04300	0.00000	
42	49	0.07150	0.32300	0.04300	0.00000	
45	49	0.06840	0.18600	0.02220	0.00000	
48	49	0.01790	0.05050	0.00629	0.00000	
49	50	0.02670	0.07520	0.00937	0.00000	
49	51	0.04860	0.13700	0.01710	0.00000	
51	52	0.02030	0.05880	0.00698	0.00000	
52	53	0.04050	0.16350	0.02029	0.00000	
53	54	0.02630	0.12200	0.01550	0.00000	
49	54	0.07300	0.28900	0.03690	0.00000	
49	54	0.08690	0.29100	0.03650	0.00000	

Table B.66
System (branch) setting data (Part 3)

From	To	R	X	Y/2	Tap	Remark
54	55	0.01690	0.07070	0.01010	0.00000	
54	56	0.00275	0.00955	0.00366	0.00000	
55	56	0.00488	0.01510	0.00187	0.00000	
56	57	0.03430	0.09660	0.01210	0.00000	
50	57	0.04740	0.13400	0.01660	0.00000	
56	58	0.03430	0.09660	0.01210	0.00000	
51	58	0.02550	0.07190	0.00894	0.00000	
54	59	0.05030	0.22930	0.02990	0.00000	
56	59	0.08250	0.25100	0.02845	0.00000	
56	59	0.08030	0.23900	0.02680	0.00000	
55	59	0.04739	0.21580	0.02823	0.00000	
59	60	0.03170	0.14500	0.01880	0.00000	
59	61	0.03280	0.15000	0.01940	0.00000	
60	61	0.00264	0.01350	0.00728	0.00000	
60	62	0.01230	0.05610	0.00734	0.00000	
61	62	0.00824	0.03760	0.00490	0.00000	
63	64	0.00172	0.02000	0.10800	0.00000	
38	65	0.00901	0.09860	0.52300	0.00000	
64	65	0.00269	0.03020	0.19000	0.00000	
49	66	0.01800	0.09190	0.01240	0.00000	
49	66	0.01800	0.09190	0.01240	0.00000	
62	66	0.04820	0.21800	0.02890	0.00000	
62	67	0.02580	0.11700	0.01550	0.00000	
66	67	0.02240	0.10150	0.01341	0.00000	
65	68	0.00138	0.01600	0.31900	0.00000	
47	69	0.08440	0.27780	0.03546	0.00000	
49	69	0.09850	0.32400	0.04140	0.00000	
69	70	0.03000	0.12700	0.06100	0.00000	
24	70	0.00221	0.41150	0.05099	0.00000	
70	71	0.00882	0.03550	0.00439	0.00000	
24	72	0.04880	0.19600	0.02440	0.00000	
71	72	0.04460	0.18000	0.02222	0.00000	
71	73	0.00866	0.04540	0.00589	0.00000	
70	74	0.04010	0.13230	0.01684	0.00000	
70	75	0.04280	0.14100	0.01800	0.00000	
69	75	0.04050	0.12200	0.06200	0.00000	

Table B.67
System (branch) setting data (Part 4)

From	To	R	X	Y/2	Tap	Remark
74	75	0.01230	0.04060	0.00517	0.00000	
76	77	0.04440	0.14800	0.01840	0.00000	
69	77	0.03090	0.10100	0.05190	0.00000	
75	77	0.06010	0.19990	0.02489	0.00000	
77	78	0.00376	0.01240	0.00632	0.00000	
78	79	0.00546	0.02440	0.00324	0.00000	
77	80	0.01700	0.04850	0.02360	0.00000	
77	80	0.02940	0.10500	0.01140	0.00000	
79	80	0.01560	0.07040	0.00935	0.00000	
68	81	0.00175	0.02020	0.40400	0.00000	
77	82	0.02980	0.08530	0.04087	0.00000	
82	83	0.01120	0.03665	0.01898	0.00000	
83	84	0.06250	0.13200	0.01290	0.00000	
83	85	0.04300	0.14800	0.01740	0.00000	
84	85	0.03020	0.06410	0.00617	0.00000	
85	86	0.03500	0.12300	0.01380	0.00000	
86	87	0.02828	0.20740	0.02225	0.00000	
85	88	0.02000	0.10200	0.01380	0.00000	
85	89	0.02390	0.17300	0.02350	0.00000	
88	89	0.01390	0.07120	0.00967	0.00000	
89	90	0.05180	0.18800	0.02640	0.00000	
89	90	0.02380	0.09970	0.05300	0.00000	
90	91	0.02540	0.08360	0.01070	0.00000	
89	92	0.00990	0.05050	0.02740	0.00000	
89	92	0.03930	0.15810	0.02070	0.00000	
91	92	0.03870	0.12720	0.01634	0.00000	
92	93	0.02580	0.08480	0.01090	0.00000	
92	94	0.04810	0.15800	0.02030	0.00000	
93	94	0.02230	0.07320	0.00938	0.00000	
94	95	0.01320	0.04340	0.00555	0.00000	
80	96	0.03560	0.18200	0.02470	0.00000	
82	96	0.01620	0.05300	0.02720	0.00000	
94	96	0.02690	0.08690	0.01150	0.00000	
80	97	0.01830	0.09340	0.01270	0.00000	
80	98	0.02380	0.10800	0.01430	0.00000	
80	99	0.04540	0.20600	0.02730	0.00000	

Table B.68
System (branch) setting data (Part 5)

From	To	R	X	Y/2	Tap	Remark
92	100	0.06480	0.29500	0.02360	0.00000	
94	100	0.01780	0.05800	0.03020	0.00000	
95	96	0.01710	0.05470	0.00737	0.00000	
96	97	0.01730	0.08850	0.01200	0.00000	
98	100	0.03970	0.17900	0.02380	0.00000	
99	100	0.01800	0.08130	0.01080	0.00000	
100	101	0.02770	0.12620	0.01640	0.00000	
92	102	0.01230	0.05590	0.00732	0.00000	
101	102	0.02460	0.11200	0.01470	0.00000	
100	103	0.01600	0.05250	0.02680	0.00000	
100	104	0.04510	0.20400	0.02705	0.00000	
103	104	0.04660	0.15840	0.02035	0.00000	
103	105	0.05350	0.16250	0.02040	0.00000	
100	106	0.06050	0.22900	0.03100	0.00000	
104	105	0.00994	0.03780	0.00493	0.00000	
105	106	0.01400	0.05470	0.00717	0.00000	
105	107	0.05300	0.18300	0.02360	0.00000	
105	108	0.02610	0.07030	0.00922	0.00000	
106	107	0.05300	0.18300	0.02360	0.00000	
108	109	0.01050	0.02880	0.00380	0.00000	
103	110	0.03906	0.18130	0.02305	0.00000	
109	110	0.02780	0.07620	0.01010	0.00000	
110	111	0.02200	0.07550	0.01000	0.00000	
110	112	0.02470	0.06400	0.03100	0.00000	
17	113	0.00913	0.03010	0.00384	0.00000	
32	113	0.06150	0.20300	0.02590	0.00000	
32	114	0.01350	0.06120	0.00814	0.00000	
27	115	0.01640	0.07410	0.00986	0.00000	
114	115	0.00230	0.01040	0.00138	0.00000	
68	116	0.00034	0.00405	0.08200	0.00000	
12	117	0.03290	0.14000	0.01790	0.00000	
75	118	0.01450	0.04810	0.00599	0.00000	
76	118	0.01640	0.05440	0.00678	0.00000	
120	123	0.00000	0.02670	0.00000	0.98500	
140	141	0.00000	0.03820	0.00000	0.96000	
132	145	0.00000	0.03880	0.00000	0.96000	

Table B.69
System (branch) setting data (Part 6)

From	To	R	X	Y/2	Tap	Remark
152	153	0.00000	0.03750	0.00000	0.93500	
174	178	0.00000	0.03860	0.00000	0.96000	
176	179	0.00000	0.02680	0.00000	0.98500	
181	180	0.00000	0.03700	0.00000	0.93500	
184	183	0.00000	0.03700	0.00000	0.93500	
195	196	0.00000	0.03700	0.00000	0.93500	
5	120	0.00000	0.00000	0.00000	0.00000	59
25	140	0.00000	0.00000	0.00000	0.00000	59
17	132	0.00000	0.00000	0.00000	0.00000	59
37	152	0.00000	0.00000	0.00000	0.00000	59
59	174	0.00000	0.00000	0.00000	0.00000	59
61	176	0.00000	0.00000	0.00000	0.00000	59
66	181	0.00000	0.00000	0.00000	0.00000	59
69	184	0.00000	0.00000	0.00000	0.00000	59
80	195	0.00000	0.00000	0.00000	0.00000	59
123	8	0.00000	0.00000	0.00000	0.00000	59
141	26	0.00000	0.00000	0.00000	0.00000	59
145	30	0.00000	0.00000	0.00000	0.00000	59
153	38	0.00000	0.00000	0.00000	0.00000	59
178	63	0.00000	0.00000	0.00000	0.00000	59
179	64	0.00000	0.00000	0.00000	0.00000	59
180	65	0.00000	0.00000	0.00000	0.00000	59
183	68	0.00000	0.00000	0.00000	0.00000	59
196	81	0.00000	0.00000	0.00000	0.00000	59
1	201	0.00000	0.00000	0.00000	0.00000	CB
201	301	0.00000	0.00000	0.00000	0.00000	81
301	401	0.00000	0.00000	0.00000	0.00000	78
401	501	0.00000	0.00000	0.00000	0.00000	59
4	204	0.00000	0.00000	0.00000	0.00000	CB
204	304	0.00000	0.00000	0.00000	0.00000	81
304	404	0.00000	0.00000	0.00000	0.00000	78
404	504	0.00000	0.00000	0.00000	0.00000	59
6	206	0.00000	0.00000	0.00000	0.00000	CB
206	306	0.00000	0.00000	0.00000	0.00000	81
306	406	0.00000	0.00000	0.00000	0.00000	78
406	506	0.00000	0.00000	0.00000	0.00000	59

Table B.70
System (branch) setting data (Part 7)

From	To	R	X	Y/2	Tap	Remark
8	208	0.00000	0.00000	0.00000	0.00000	CB
208	308	0.00000	0.00000	0.00000	0.00000	81
308	408	0.00000	0.00000	0.00000	0.00000	78
408	508	0.00000	0.00000	0.00000	0.00000	59
10	210	0.00000	0.00000	0.00000	0.00000	CB
210	310	0.00000	0.00000	0.00000	0.00000	81
310	410	0.00000	0.00000	0.00000	0.00000	78
410	510	0.00000	0.00000	0.00000	0.00000	59
12	212	0.00000	0.00000	0.00000	0.00000	CB
212	312	0.00000	0.00000	0.00000	0.00000	81
312	412	0.00000	0.00000	0.00000	0.00000	78
412	512	0.00000	0.00000	0.00000	0.00000	59
15	215	0.00000	0.00000	0.00000	0.00000	CB
215	315	0.00000	0.00000	0.00000	0.00000	81
315	415	0.00000	0.00000	0.00000	0.00000	78
415	515	0.00000	0.00000	0.00000	0.00000	59
18	218	0.00000	0.00000	0.00000	0.00000	CB
218	318	0.00000	0.00000	0.00000	0.00000	81
318	418	0.00000	0.00000	0.00000	0.00000	78
418	518	0.00000	0.00000	0.00000	0.00000	59
19	219	0.00000	0.00000	0.00000	0.00000	CB
219	319	0.00000	0.00000	0.00000	0.00000	81
319	419	0.00000	0.00000	0.00000	0.00000	78
419	519	0.00000	0.00000	0.00000	0.00000	59
24	224	0.00000	0.00000	0.00000	0.00000	CB
224	324	0.00000	0.00000	0.00000	0.00000	81
324	424	0.00000	0.00000	0.00000	0.00000	78
424	524	0.00000	0.00000	0.00000	0.00000	59
25	225	0.00000	0.00000	0.00000	0.00000	CB
225	325	0.00000	0.00000	0.00000	0.00000	81
325	425	0.00000	0.00000	0.00000	0.00000	78
425	525	0.00000	0.00000	0.00000	0.00000	59
26	226	0.00000	0.00000	0.00000	0.00000	CB
226	326	0.00000	0.00000	0.00000	0.00000	81
326	426	0.00000	0.00000	0.00000	0.00000	78
426	526	0.00000	0.00000	0.00000	0.00000	59

Table B.71
System (branch) setting data (Part 8)

From	To	R	X	Y/2	Tap	Remark
27	227	0.00000	0.00000	0.00000	0.00000	CB
227	327	0.00000	0.00000	0.00000	0.00000	81
327	427	0.00000	0.00000	0.00000	0.00000	78
427	527	0.00000	0.00000	0.00000	0.00000	59
31	231	0.00000	0.00000	0.00000	0.00000	CB
231	331	0.00000	0.00000	0.00000	0.00000	81
331	431	0.00000	0.00000	0.00000	0.00000	78
431	531	0.00000	0.00000	0.00000	0.00000	59
32	232	0.00000	0.00000	0.00000	0.00000	CB
232	332	0.00000	0.00000	0.00000	0.00000	81
332	432	0.00000	0.00000	0.00000	0.00000	78
432	532	0.00000	0.00000	0.00000	0.00000	59
34	234	0.00000	0.00000	0.00000	0.00000	CB
234	334	0.00000	0.00000	0.00000	0.00000	81
334	434	0.00000	0.00000	0.00000	0.00000	78
434	534	0.00000	0.00000	0.00000	0.00000	59
36	236	0.00000	0.00000	0.00000	0.00000	CB
236	336	0.00000	0.00000	0.00000	0.00000	81
336	436	0.00000	0.00000	0.00000	0.00000	78
436	536	0.00000	0.00000	0.00000	0.00000	59
40	240	0.00000	0.00000	0.00000	0.00000	CB
240	340	0.00000	0.00000	0.00000	0.00000	81
340	440	0.00000	0.00000	0.00000	0.00000	78
440	540	0.00000	0.00000	0.00000	0.00000	59
42	242	0.00000	0.00000	0.00000	0.00000	CB
242	342	0.00000	0.00000	0.00000	0.00000	81
342	442	0.00000	0.00000	0.00000	0.00000	78
442	542	0.00000	0.00000	0.00000	0.00000	59
46	246	0.00000	0.00000	0.00000	0.00000	CB
246	346	0.00000	0.00000	0.00000	0.00000	81
346	446	0.00000	0.00000	0.00000	0.00000	78
446	546	0.00000	0.00000	0.00000	0.00000	59
49	249	0.00000	0.00000	0.00000	0.00000	CB
249	349	0.00000	0.00000	0.00000	0.00000	81
349	449	0.00000	0.00000	0.00000	0.00000	78
449	549	0.00000	0.00000	0.00000	0.00000	59

Table B.72
System (branch) setting data (Part 9)

From	To	R	X	Y/2	Tap	Remark
54	254	0.00000	0.00000	0.00000	0.00000	CB
254	354	0.00000	0.00000	0.00000	0.00000	81
354	454	0.00000	0.00000	0.00000	0.00000	78
454	554	0.00000	0.00000	0.00000	0.00000	59
55	255	0.00000	0.00000	0.00000	0.00000	CB
255	355	0.00000	0.00000	0.00000	0.00000	81
355	455	0.00000	0.00000	0.00000	0.00000	78
455	555	0.00000	0.00000	0.00000	0.00000	59
56	256	0.00000	0.00000	0.00000	0.00000	CB
256	356	0.00000	0.00000	0.00000	0.00000	81
356	456	0.00000	0.00000	0.00000	0.00000	78
456	556	0.00000	0.00000	0.00000	0.00000	59
59	259	0.00000	0.00000	0.00000	0.00000	CB
259	359	0.00000	0.00000	0.00000	0.00000	81
359	459	0.00000	0.00000	0.00000	0.00000	78
459	559	0.00000	0.00000	0.00000	0.00000	59
61	261	0.00000	0.00000	0.00000	0.00000	CB
261	361	0.00000	0.00000	0.00000	0.00000	81
361	461	0.00000	0.00000	0.00000	0.00000	78
461	561	0.00000	0.00000	0.00000	0.00000	59
62	262	0.00000	0.00000	0.00000	0.00000	CB
262	362	0.00000	0.00000	0.00000	0.00000	81
362	462	0.00000	0.00000	0.00000	0.00000	78
462	562	0.00000	0.00000	0.00000	0.00000	59
65	265	0.00000	0.00000	0.00000	0.00000	CB
265	365	0.00000	0.00000	0.00000	0.00000	81
365	465	0.00000	0.00000	0.00000	0.00000	78
465	565	0.00000	0.00000	0.00000	0.00000	59
66	266	0.00000	0.00000	0.00000	0.00000	CB
266	366	0.00000	0.00000	0.00000	0.00000	81
366	466	0.00000	0.00000	0.00000	0.00000	78
466	566	0.00000	0.00000	0.00000	0.00000	59
69	269	0.00000	0.00000	0.00000	0.00000	CB
269	369	0.00000	0.00000	0.00000	0.00000	81
369	469	0.00000	0.00000	0.00000	0.00000	78
469	569	0.00000	0.00000	0.00000	0.00000	59

Table B.73
System (branch) setting data (Part 10)

From	To	R	X	Y/2	Tap	Remark
70	270	0.00000	0.00000	0.00000	0.00000	CB
270	370	0.00000	0.00000	0.00000	0.00000	81
370	470	0.00000	0.00000	0.00000	0.00000	78
470	570	0.00000	0.00000	0.00000	0.00000	59
72	272	0.00000	0.00000	0.00000	0.00000	CB
272	372	0.00000	0.00000	0.00000	0.00000	81
372	472	0.00000	0.00000	0.00000	0.00000	78
472	572	0.00000	0.00000	0.00000	0.00000	59
73	273	0.00000	0.00000	0.00000	0.00000	CB
273	373	0.00000	0.00000	0.00000	0.00000	81
373	473	0.00000	0.00000	0.00000	0.00000	78
473	573	0.00000	0.00000	0.00000	0.00000	59
74	274	0.00000	0.00000	0.00000	0.00000	CB
274	374	0.00000	0.00000	0.00000	0.00000	81
374	474	0.00000	0.00000	0.00000	0.00000	78
474	574	0.00000	0.00000	0.00000	0.00000	59
76	276	0.00000	0.00000	0.00000	0.00000	CB
276	376	0.00000	0.00000	0.00000	0.00000	81
376	476	0.00000	0.00000	0.00000	0.00000	78
476	576	0.00000	0.00000	0.00000	0.00000	59
77	277	0.00000	0.00000	0.00000	0.00000	CB
277	377	0.00000	0.00000	0.00000	0.00000	81
377	477	0.00000	0.00000	0.00000	0.00000	78
477	577	0.00000	0.00000	0.00000	0.00000	59
80	280	0.00000	0.00000	0.00000	0.00000	CB
280	380	0.00000	0.00000	0.00000	0.00000	81
380	480	0.00000	0.00000	0.00000	0.00000	78
480	580	0.00000	0.00000	0.00000	0.00000	59
85	285	0.00000	0.00000	0.00000	0.00000	CB
285	385	0.00000	0.00000	0.00000	0.00000	81
385	485	0.00000	0.00000	0.00000	0.00000	78
485	585	0.00000	0.00000	0.00000	0.00000	59
87	287	0.00000	0.00000	0.00000	0.00000	CB
287	387	0.00000	0.00000	0.00000	0.00000	81
387	487	0.00000	0.00000	0.00000	0.00000	78
487	587	0.00000	0.00000	0.00000	0.00000	59

Table B.74
System (branch) setting data (Part 11)

From	To	R	X	Y/2	Tap	Remark
89	289	0.00000	0.00000	0.00000	0.00000	CB
289	389	0.00000	0.00000	0.00000	0.00000	81
389	489	0.00000	0.00000	0.00000	0.00000	78
489	589	0.00000	0.00000	0.00000	0.00000	59
90	290	0.00000	0.00000	0.00000	0.00000	CB
290	390	0.00000	0.00000	0.00000	0.00000	81
390	490	0.00000	0.00000	0.00000	0.00000	78
490	590	0.00000	0.00000	0.00000	0.00000	59
91	291	0.00000	0.00000	0.00000	0.00000	CB
291	391	0.00000	0.00000	0.00000	0.00000	81
391	491	0.00000	0.00000	0.00000	0.00000	78
491	591	0.00000	0.00000	0.00000	0.00000	59
92	292	0.00000	0.00000	0.00000	0.00000	CB
292	392	0.00000	0.00000	0.00000	0.00000	81
392	492	0.00000	0.00000	0.00000	0.00000	78
492	592	0.00000	0.00000	0.00000	0.00000	59
99	299	0.00000	0.00000	0.00000	0.00000	CB
299	399	0.00000	0.00000	0.00000	0.00000	81
399	499	0.00000	0.00000	0.00000	0.00000	78
499	599	0.00000	0.00000	0.00000	0.00000	59
100	600	0.00000	0.00000	0.00000	0.00000	CB
600	700	0.00000	0.00000	0.00000	0.00000	81
700	800	0.00000	0.00000	0.00000	0.00000	78
800	900	0.00000	0.00000	0.00000	0.00000	59
103	603	0.00000	0.00000	0.00000	0.00000	CB
603	703	0.00000	0.00000	0.00000	0.00000	81
703	803	0.00000	0.00000	0.00000	0.00000	78
803	903	0.00000	0.00000	0.00000	0.00000	59
104	604	0.00000	0.00000	0.00000	0.00000	CB
604	704	0.00000	0.00000	0.00000	0.00000	81
704	804	0.00000	0.00000	0.00000	0.00000	78
804	904	0.00000	0.00000	0.00000	0.00000	59
105	605	0.00000	0.00000	0.00000	0.00000	CB
605	705	0.00000	0.00000	0.00000	0.00000	81
705	805	0.00000	0.00000	0.00000	0.00000	78
805	905	0.00000	0.00000	0.00000	0.00000	59

Table B.75
System (branch) setting data (Part 12)

From	To	R	X	Y/2	Tap	Remark
107	607	0.00000	0.00000	0.00000	0.00000	CB
607	707	0.00000	0.00000	0.00000	0.00000	81
707	807	0.00000	0.00000	0.00000	0.00000	78
807	907	0.00000	0.00000	0.00000	0.00000	59
110	610	0.00000	0.00000	0.00000	0.00000	CB
610	710	0.00000	0.00000	0.00000	0.00000	81
710	810	0.00000	0.00000	0.00000	0.00000	78
810	910	0.00000	0.00000	0.00000	0.00000	59
111	611	0.00000	0.00000	0.00000	0.00000	CB
611	711	0.00000	0.00000	0.00000	0.00000	81
711	811	0.00000	0.00000	0.00000	0.00000	78
811	911	0.00000	0.00000	0.00000	0.00000	59
112	612	0.00000	0.00000	0.00000	0.00000	CB
612	712	0.00000	0.00000	0.00000	0.00000	81
712	812	0.00000	0.00000	0.00000	0.00000	78
812	912	0.00000	0.00000	0.00000	0.00000	59
113	613	0.00000	0.00000	0.00000	0.00000	CB
613	713	0.00000	0.00000	0.00000	0.00000	81
713	813	0.00000	0.00000	0.00000	0.00000	78
813	913	0.00000	0.00000	0.00000	0.00000	59
116	616	0.00000	0.00000	0.00000	0.00000	CB
616	716	0.00000	0.00000	0.00000	0.00000	81
716	816	0.00000	0.00000	0.00000	0.00000	78
816	916	0.00000	0.00000	0.00000	0.00000	59

Table B.76
Power flow condition setting data (Part 1)

Node	V magnitude	PG	QG	PL	QL	QC	Name
1	0.0000	0.0000	0.0000	0.5100	0.2700	0.0000	Riverside1
2	0.0000	0.0000	0.0000	0.2000	0.0900	0.0000	Pokagon
3	0.0000	0.0000	0.0000	0.3900	0.1000	0.0000	HickoryCk
4	0.0000	0.0000	0.0000	0.3900	0.1200	0.0000	NCarlisle1
5	0.0000	0.0000	0.0000	0.0000	0.0000	-0.4000	Olive
6	0.0000	0.0000	0.0000	0.5200	0.2200	0.0000	Kankakee1
7	0.0000	0.0000	0.0000	0.1900	0.0200	0.0000	JacksonRd
8	0.0000	0.0000	0.0000	0.2800	0.0000	0.0000	Olive1
9	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Beguine
10	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Breed1
11	0.0000	0.0000	0.0000	0.7000	0.2300	0.0000	SouthBend
12	0.0000	0.0000	0.0000	0.4700	0.1000	0.0000	TwnBranch1
13	0.0000	0.0000	0.0000	0.3400	0.1600	0.0000	Concord
14	0.0000	0.0000	0.0000	0.1400	0.0100	0.0000	GoshenJct
15	0.0000	0.0000	0.0000	0.9000	0.3000	0.0000	FortWayne1
16	0.0000	0.0000	0.0000	0.2500	0.1000	0.0000	N. E.
17	0.0000	0.0000	0.0000	0.1100	0.0300	0.0000	Sorenson
18	0.0000	0.0000	0.0000	0.6000	0.3400	0.0000	McKinley1
19	0.0000	0.0000	0.0000	0.4500	0.2500	0.0000	Lincoln1
20	0.0000	0.0000	0.0000	0.1800	0.0300	0.0000	Adams
21	0.0000	0.0000	0.0000	0.1400	0.0800	0.0000	Jay
22	0.0000	0.0000	0.0000	0.1000	0.0500	0.0000	Randolph
23	0.0000	0.0000	0.0000	0.0700	0.0300	0.0000	CollgeCnr
24	0.0000	0.0000	0.0000	0.1300	0.0000	0.0000	Trenton1
25	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	TannersCk1
26	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	TannersCk3
27	0.0000	0.0000	0.0000	0.7100	0.1300	0.0000	Madison1
28	0.0000	0.0000	0.0000	0.1700	0.0700	0.0000	Mullin
29	0.0000	0.0000	0.0000	0.2400	0.0400	0.0000	Grant
30	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Sorenson
31	0.0000	0.0000	0.0000	0.4300	0.2700	0.0000	DeerCreek1
32	0.0000	0.0000	0.0000	0.5900	0.2300	0.0000	Delaware1
33	0.0000	0.0000	0.0000	0.2300	0.0900	0.0000	Haviland
34	0.0000	0.0000	0.0000	0.5900	0.2600	0.1400	Rockhill1
35	0.0000	0.0000	0.0000	0.3300	0.0900	0.0000	West Lima

Table B.77
Power flow condition setting data (Part 2)

Node	V magnitude	PG	QG	PL	QL	QC	Name
36	0.0000	0.0000	0.0000	0.3100	0.1700	0.0000	Sterling1
37	0.0000	0.0000	0.0000	0.0000	0.0000	-0.2500	East Lima
38	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	East Lima
39	0.0000	0.0000	0.0000	0.2700	0.1100	0.0000	NwLiberty
40	0.0000	0.0000	0.0000	0.6600	0.2300	0.0000	West End1
41	0.0000	0.0000	0.0000	0.3700	0.1000	0.0000	S. Tiffin
42	0.0000	0.0000	0.0000	0.9600	0.2300	0.0000	Howard1
43	0.0000	0.0000	0.0000	0.1800	0.0700	0.0000	S. Kenton
44	0.0000	0.0000	0.0000	0.1600	0.0800	0.1000	WMtVernon
45	0.0000	0.0000	0.0000	0.5300	0.2200	0.1000	N. Newark
46	0.0000	0.0000	0.0000	0.2800	0.1000	0.1000	W.Lancstr1
47	0.0000	0.0000	0.0000	0.3400	0.0000	0.0000	Crooksvil
48	0.0000	0.0000	0.0000	0.2000	0.1100	0.1500	Zanesvile
49	0.0000	0.0000	0.0000	0.8700	0.3000	0.0000	Philo1
50	0.0000	0.0000	0.0000	0.1700	0.0400	0.0000	W.Cambrdg
51	0.0000	0.0000	0.0000	0.1700	0.0800	0.0000	Newcmrstn
52	0.0000	0.0000	0.0000	0.1800	0.0500	0.0000	SCoshoctn
53	0.0000	0.0000	0.0000	0.2300	0.1100	0.0000	Wooster
54	0.0000	0.0000	0.0000	1.1300	0.3200	0.0000	Torrey1
55	0.0000	0.0000	0.0000	0.6300	0.2200	0.0000	Wagenhals1
56	0.0000	0.0000	0.0000	0.8400	0.1800	0.0000	Sunnyside1
57	0.0000	0.0000	0.0000	0.1200	0.0300	0.0000	WNwPhila1
58	0.0000	0.0000	0.0000	0.1200	0.0300	0.0000	WNwPhila2
59	0.0000	0.0000	0.0000	2.7700	1.1300	0.0000	Tidd1
60	0.0000	0.0000	0.0000	0.7800	0.0300	0.0000	SW Kammer
61	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	W. Kammer1
62	0.0000	0.0000	0.0000	0.7700	0.1400	0.0000	Natrium1
63	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Tidd
64	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Kammer
65	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Muskingum1
66	0.0000	0.0000	0.0000	0.3900	0.1800	0.0000	Muskingum1
67	0.0000	0.0000	0.0000	0.2800	0.0700	0.0000	Summerfld
68	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Sporn
69	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Sporn1
70	0.0000	0.0000	0.0000	0.6600	0.2000	0.0000	Portsmoth1

Table B.78
Power flow condition setting data (Part 3)

Node	V magnitude	PG	QG	PL	QL	QC	Name
71	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	NPortsmth
72	0.0000	0.0000	0.0000	0.1200	0.0000	0.0000	Hillsboro1
73	0.0000	0.0000	0.0000	0.0600	0.0000	0.0000	Sargents1
74	0.0000	0.0000	0.0000	0.6800	0.2700	0.1200	Bellefont1
75	0.0000	0.0000	0.0000	0.4700	0.1100	0.0000	Sth Point
76	0.0000	0.0000	0.0000	0.6800	0.3600	0.0000	Darrah1
77	0.0000	0.0000	0.0000	0.6100	0.2800	0.0000	Turner1
78	0.0000	0.0000	0.0000	0.7100	0.2600	0.0000	Chemical
79	0.0000	0.0000	0.0000	0.3900	0.3200	0.2000	CapitolHl
80	0.0000	0.0000	0.0000	1.3000	0.2600	0.0000	Cabin Crk1
81	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Kanawha
82	0.0000	0.0000	0.0000	0.5400	0.2700	0.2000	Logan
83	0.0000	0.0000	0.0000	0.2000	0.1000	0.1000	Sprigg
84	0.0000	0.0000	0.0000	0.1100	0.0700	0.0000	BetsyLayn
85	0.0000	0.0000	0.0000	0.2400	0.1500	0.0000	BeaverCrk1
86	0.0000	0.0000	0.0000	0.2100	0.1000	0.0000	Hazard
87	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Pineville1
88	0.0000	0.0000	0.0000	0.4800	0.1000	0.0000	Fremont
89	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	ClinchRvr1
90	0.0000	0.0000	0.0000	1.6300	0.4200	0.0000	Holston1
91	0.0000	0.0000	0.0000	0.1000	0.0000	0.0000	HolstonTP1
92	0.0000	0.0000	0.0000	0.6500	0.1000	0.0000	Saltville1
93	0.0000	0.0000	0.0000	0.1200	0.0700	0.0000	Tazewell
94	0.0000	0.0000	0.0000	0.3000	0.1600	0.0000	Switchbak
95	0.0000	0.0000	0.0000	0.4200	0.3100	0.0000	Caldwell
96	0.0000	0.0000	0.0000	0.3800	0.1500	0.0000	Baileysvl
97	0.0000	0.0000	0.0000	0.1500	0.0900	0.0000	Sundial
98	0.0000	0.0000	0.0000	0.3400	0.0800	0.0000	Bradley
99	0.0000	0.0000	0.0000	0.4200	0.0000	0.0000	Hinton1
100	0.0000	0.0000	0.0000	0.3700	0.1800	0.0000	Glen Lyn1
101	0.0000	0.0000	0.0000	0.2200	0.1500	0.0000	Wythe
102	0.0000	0.0000	0.0000	0.0500	0.0300	0.0000	Smyth
103	0.0000	0.0000	0.0000	0.2300	0.1600	0.0000	Claytor1
104	0.0000	0.0000	0.0000	0.3800	0.2500	0.0000	Hancock1
105	0.0000	0.0000	0.0000	0.3100	0.2600	0.2000	Roanoke1

Table B.79
Power flow condition setting data (Part 4)

Node	V magnitude	PG	QG	PL	QL	QC	Name
106	0.0000	0.0000	0.0000	0.4300	0.1600	0.0000	Cloverdle
107	0.0000	0.0000	0.0000	0.5000	0.1200	0.0600	Reusens1
108	0.0000	0.0000	0.0000	0.0200	0.0100	0.0000	Blaine
109	0.0000	0.0000	0.0000	0.0800	0.0300	0.0000	Franklin
110	0.0000	0.0000	0.0000	0.3900	0.3000	0.0600	Fieldale1
111	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	Dan River1
112	0.0000	0.0000	0.0000	0.6800	0.1300	0.0000	Danville1
113	0.0000	0.0000	0.0000	0.0600	0.0000	0.0000	DeerCk TP1
114	0.0000	0.0000	0.0000	0.0800	0.0300	0.0000	W Medford
115	0.0000	0.0000	0.0000	0.2200	0.0700	0.0000	Medford
116	0.0000	0.0000	0.0000	1.8400	0.0000	0.0000	Kyger Crk1
117	0.0000	0.0000	0.0000	0.2000	0.0800	0.0000	Corey
118	0.0000	0.0000	0.0000	0.3300	0.1500	0.0000	WHuntngdn
120	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
123	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
132	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
140	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
141	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
145	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
152	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
153	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
174	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
176	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
178	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
179	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
180	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
181	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
183	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
184	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
195	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
196	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
201	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
204	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
206	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
208	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.80
Power flow condition setting data (Part 5)

Node	V magnitude	PG	QG	PL	QL	QC	Name
210	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
212	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
215	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
218	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
219	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
224	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
225	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
226	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
227	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
231	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
232	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
234	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
236	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
240	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
242	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
246	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
249	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
254	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
255	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
256	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
259	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
261	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
262	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
265	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
266	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
269	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
270	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
272	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
273	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
274	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
276	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
277	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
280	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
285	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
287	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.81
Power flow condition setting data (Part 6)

Node	V magnitude	PG	QG	PL	QL	QC	Name
289	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
290	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
291	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
292	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
299	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
301	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
304	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
306	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
308	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
310	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
312	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
315	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
318	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
319	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
324	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
325	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
326	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
327	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
331	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
332	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
334	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
336	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
340	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
342	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
346	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
349	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
354	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
355	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
356	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
359	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
361	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
362	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
365	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
366	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
369	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.82
Power flow condition setting data (Part 7)

Node	V magnitude	PG	QG	PL	QL	QC	Name
370	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
372	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
373	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
374	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
376	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
377	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
380	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
385	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
387	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
389	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
390	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
391	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
392	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
399	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
401	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
404	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
406	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
408	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
410	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
412	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
415	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
418	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
419	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
424	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
425	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
426	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
427	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
431	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
432	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
434	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
436	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
440	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
442	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
446	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
449	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.83
Power flow condition setting data (Part 8)

Node	V magnitude	PG	QG	PL	QL	QC	Name
454	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
455	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
456	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
459	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
461	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
462	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
465	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
466	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
469	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
470	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
472	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
473	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
474	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
476	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
477	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
480	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
485	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
487	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
489	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
490	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
491	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
492	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
499	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
501	0.9550	0.0000	-0.0310	0.0000	0.0000	0.0000	Riverside2
504	0.9980	0.0000	-0.1500	0.0000	0.0000	0.0000	NCarlisle2
506	0.9900	0.0000	0.1593	0.0000	0.0000	0.0000	Kankakee2
508	1.0150	0.0000	0.6276	0.0000	0.0000	0.0000	Olive2
510	1.0500	4.5000	0.0000	0.0000	0.0000	0.0000	Breed2
512	0.9900	0.8500	0.0000	0.0000	0.0000	0.0000	TwnBranch2
515	0.9700	0.0000	0.0306	0.0000	0.0000	0.0000	FortWayne2
518	0.9730	0.0000	0.2553	0.0000	0.0000	0.0000	McKinley2
519	0.9620	0.0000	-0.0800	0.0000	0.0000	0.0000	Lincoln2
524	0.9920	0.0000	-0.1528	0.0000	0.0000	0.0000	Trenton2
525	1.0500	2.2000	0.0000	0.0000	0.0000	0.0000	TannersCk2
526	1.0150	3.1400	0.0000	0.0000	0.0000	0.0000	TannersCk4

Table B.84
Power flow condition setting data (Part 9)

Node	V magnitude	PG	QG	PL	QL	QC	Name
527	0.9680	0.0000	0.0283	0.0000	0.0000	0.0000	Madison2
531	0.9670	0.0700	0.0000	0.0000	0.0000	0.0000	DeerCreek2
532	0.9630	0.0000	-0.1400	0.0000	0.0000	0.0000	Delaware2
534	0.9840	0.0000	-0.0800	0.0000	0.0000	0.0000	Rockhill2
536	0.9800	0.0000	-0.0125	0.0000	0.0000	0.0000	Sterling2
540	0.9700	0.0000	0.2689	0.0000	0.0000	0.0000	West End2
542	0.9850	0.0000	0.4100	0.0000	0.0000	0.0000	Howard2
546	1.0050	0.1900	0.0000	0.0000	0.0000	0.0000	W.Lancstr2
549	1.0250	2.0400	0.0000	0.0000	0.0000	0.0000	Philo2
554	0.9550	0.4800	0.0000	0.0000	0.0000	0.0000	Torrey2
555	0.9520	0.0000	0.0466	0.0000	0.0000	0.0000	Wagenhals2
556	0.9540	0.0000	-0.0229	0.0000	0.0000	0.0000	Sunnyside2
559	0.9850	1.5500	0.0000	0.0000	0.0000	0.0000	Tidd2
561	0.9950	1.6000	0.0000	0.0000	0.0000	0.0000	W. Kammer2
562	0.9980	0.0000	0.0126	0.0000	0.0000	0.0000	Natrium2
565	1.0050	3.9100	0.0000	0.0000	0.0000	0.0000	Muskingum2
566	1.0500	3.9200	0.0000	0.0000	0.0000	0.0000	Muskingum2
569	1.0350	0.0000	0.0000	0.0000	0.0000	0.0000	Sporn2
570	0.9840	0.0000	0.0966	0.0000	0.0000	0.0000	Portsmoth2
572	0.9800	0.0000	-0.1113	0.0000	0.0000	0.0000	Hillsboro2
573	0.9910	0.0000	0.0965	0.0000	0.0000	0.0000	Sargents2
574	0.9580	0.0000	-0.0563	0.0000	0.0000	0.0000	Bellefont2
576	0.9430	0.0000	0.0527	0.0000	0.0000	0.0000	Darrah2
577	1.0060	0.0000	0.1194	0.0000	0.0000	0.0000	Turner2
580	1.0400	4.7700	0.0000	0.0000	0.0000	0.0000	Cabin Crk2
585	0.9850	0.0000	-0.0577	0.0000	0.0000	0.0000	BeaverCrk2
587	1.0150	0.0400	0.0000	0.0000	0.0000	0.0000	Pineville2
589	1.0050	6.0700	0.0000	0.0000	0.0000	0.0000	ClinchRvr2
590	0.9850	0.0000	0.5930	0.0000	0.0000	0.0000	Holston2
591	0.9800	0.0000	-0.1485	0.0000	0.0000	0.0000	HolstonTP2
592	0.9900	0.0000	-0.0300	0.0000	0.0000	0.0000	Saltville2
599	1.0100	0.0000	-0.1754	0.0000	0.0000	0.0000	Hinton2
600	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
603	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
604	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	

Table B.85
Power flow condition setting data (Part 10)

Node	V magnitude	PG	QG	PL	QL	QC	Name
605	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
607	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
610	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
611	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
612	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
613	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
616	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
700	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
703	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
704	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
705	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
707	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
710	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
711	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
712	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
713	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
716	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
800	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
803	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
804	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
805	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
807	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
810	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
811	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
812	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
813	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
816	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	
900	1.0170	2.5200	0.0000	0.0000	0.0000	0.0000	Glen Lyn2
903	1.0100	0.4000	0.0000	0.0000	0.0000	0.0000	Claytor2
904	0.9710	0.0000	0.0564	0.0000	0.0000	0.0000	Hancock2
905	0.9650	0.0000	-0.0800	0.0000	0.0000	0.0000	Roanoke2
907	0.9520	0.0000	0.0569	0.0000	0.0000	0.0000	Reusens2
910	0.9730	0.0000	0.0485	0.0000	0.0000	0.0000	Fieldale2
911	0.9800	0.3600	0.0000	0.0000	0.0000	0.0000	Dan River2
912	0.9750	0.0000	0.4151	0.0000	0.0000	0.0000	Danville2
913	0.9930	0.0000	0.0632	0.0000	0.0000	0.0000	DeerCk TP2
916	1.0050	0.0000	0.5132	0.0000	0.0000	0.0000	Kyger Crk2

Table B.86
Generator constants with implemented generator controller (part 1)

Node	AVR	OEL	PSS	GOV	GVA	GMW	GPF	MG	DG	PLM	Name
501	X				15.0	0.0	0.000	1.05	0.0	0.00	
504	X				300.0	0.0	0.000	1.05	0.0	0.00	
506	X				50.0	0.0	0.000	0.92	0.0	0.00	
508	X				300.0	0.0	0.000	1.05	0.0	0.00	
510	X	X		X	500.0	450.0	0.900	4.76	0.0	5.00	
512	X	X		X	275.3	247.8	0.900	5.48	0.0	5.00	
515	X				30.0	0.0	0.000	1.05	0.0	0.00	
518	X				50.0	0.0	0.000	1.05	0.0	0.00	
519	X				24.0	0.0	0.000	1.05	0.0	0.00	
524	X				300.0	0.0	0.000	0.92	0.0	0.00	
525	X	X		X	321.2	289.1	0.900	4.76	0.0	5.00	
526	X	X		X	2294.2	2064.7	0.900	4.60	0.0	5.00	
527	X				300.0	0.0	0.000	0.92	0.0	0.00	
531	X	X		X	688.2	619.4	0.900	4.76	0.0	5.00	
532	X				42.0	0.0	0.000	1.05	0.0	0.00	
534	X				24.0	0.0	0.000	1.05	0.0	0.00	
536	X				24.0	0.0	0.000	1.05	0.0	0.00	
540	X				300.0	0.0	0.000	0.92	0.0	0.00	
542	X				300.0	0.0	0.000	0.92	0.0	0.00	
546	X	X		X	229.4	206.5	0.900	5.48	0.0	5.00	
549	X	X		X	481.8	433.6	0.900	4.76	0.0	5.00	
554	X	X		X	668.2	619.4	0.927	4.76	0.0	5.00	
555	X				23.0	0.0	0.000	1.05	0.0	0.00	
556	X				15.0	0.0	0.000	1.05	0.0	0.00	
559	X	X		X	412.9	371.7	0.900	4.76	0.0	5.00	
561	X	X		X	688.2	619.4	0.900	4.76	0.0	5.00	
562	X				23.0	0.0	0.000	1.05	0.0	0.00	
565	X	X		X	458.8	412.9	0.900	4.76	0.0	5.00	
566	X	X		X	458.8	412.9	0.900	4.76	0.0	5.00	
569	X	X		X	688.2	619.4	0.900	4.76	0.0	5.00	Swing
570	X				32.0	0.0	0.000	1.05	0.0	0.00	
572	X				100.0	0.0	0.000	1.05	0.0	0.00	
573	X				100.0	0.0	0.000	1.05	0.0	0.00	
574	X				9.0	0.0	0.000	1.05	0.0	0.00	
576	X				23.0	0.0	0.000	1.05	0.0	0.00	
577	X				70.0	0.0	0.000	1.05	0.0	0.00	
580	X	X		X	642.4	578.1	0.900	4.76	0.0	5.00	
585	X				23.0	0.0	0.000	1.05	0.0	0.00	

Table B.87
Generator constants with implemented generator controller (part 2)

Node	AVR	OEL	PSS	GOV	GVA	GMW	GPF	MG	DG	PLM	Name
587	X	X		X	2294.2	2064.7	0.900	4.60	0.0	5.00	
589	X	X		X	688.2	619.4	0.900	4.76	0.0	5.00	
590	X				300.0	0.0	0.000	0.92	0.0	0.00	
591	X				100.0	0.0	0.000	1.05	0.0	0.00	
592	X				15.0	0.0	0.000	1.05	0.0	0.00	
599	X				100.0	0.0	0.000	1.05	0.0	0.00	
900	X	X		X	355.6	320.0	0.900	4.76	0.0	5.00	
903	X	X		X	91.8	82.6	0.900	5.48	0.0	5.00	
904	X				23.0	0.0	0.000	1.05	0.0	0.00	
905	X				23.0	0.0	0.000	1.05	0.0	0.00	
907	X				200.0	0.0	0.000	1.05	0.0	0.00	
910	X				23.0	0.0	0.000	1.05	0.0	0.00	
911	X	X		X	2294.2	2064.7	0.900	4.60	0.0	5.00	
912	X				1000.0	0.0	0.000	0.89	0.0	0.00	
913	X				200.0	0.0	0.000	0.92	0.0	0.00	
916	X				1000.0	0.0	0.000	0.89	0.0	0.00	

Table B.88
Generator constants of the used generator model (part 1)

Node	RA	XL	XD	XDD	XDDD	XFLD	XKLD	XQ	XQDD	XKLQ	TDD	TDDD	RFD	RKD	TQDD	RKQ
501	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
504	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
506	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
508	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
510	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
512	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
515	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
518	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
519	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
524	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
525	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
526	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
527	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
531	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
532	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
534	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
536	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
540	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
542	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
546	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
549	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
554	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
555	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
556	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
559	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
561	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
562	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
565	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
566	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195

Table B.89
Generator constants of the used generator model (part 2)

569	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
570	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
572	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
573	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
574	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
576	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
577	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
580	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
585	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
587	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
589	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
590	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
591	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
592	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
599	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
900	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
903	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
904	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
905	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
907	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
910	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
911	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
912	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
913	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195
916	.0017	.225	1.7	0.35	0.25	.1366	.0312	1.7	0.25	.0254	1.0	0.03	.0009	.0099	0.03	.0195

Table B.90
Initial condition of synchronous generator and condenser (part 1)

Node	AGG	VT	PG	QG	TQG	EF	CF	CDD	CQQ	FGD	FGQ
1	-19.13	0.9550	0.0000	-0.2029	0.0001	0.5938	0.5938	-0.2125	0.0001	0.9072	-0.0002
2	-14.54	0.9980	0.0000	-0.0426	0.0000	0.9254	0.9254	-0.0427	0.0000	0.9884	0.0000
3	-16.86	0.9900	0.0000	0.3254	0.0002	1.5488	1.5488	0.3287	0.0001	1.0640	-0.0002
4	-8.90	1.0150	0.0000	0.1890	0.0001	1.3316	1.3316	0.1862	0.0000	1.0569	-0.0001
5	64.58	1.0500	0.9000	-0.1025	0.9012	1.7052	1.7052	0.6818	0.5285	0.6995	-0.7796
6	1.07	0.9900	0.3088	0.3330	0.3091	1.6496	1.6496	0.4187	0.1874	1.0321	-0.2764
7	-18.81	0.9700	0.0000	0.2657	0.0001	1.4356	1.4356	0.2739	0.0001	1.0316	-0.0001
8	-18.52	0.9730	0.0000	0.5801	0.0006	1.9866	1.9866	0.5962	0.0003	1.1071	-0.0004
9	160.40	0.9620	0.0000	-0.5963	0.0006	0.0917	0.0917	0.6198	0.0069	-0.8225	-0.0102
10	-9.03	0.9920	0.0000	-0.0499	0.0000	0.9064	0.9064	-0.0503	0.0000	0.9807	0.0000
11	38.14	1.0500	0.6849	0.1625	0.6857	1.7194	1.7194	0.5389	0.3988	0.9245	-0.5882
12	12.59	1.0150	0.1369	0.0029	0.1369	1.0456	1.0456	0.0324	0.1309	0.9978	-0.1931
13	-14.58	0.9680	0.0000	0.0121	0.0000	0.9893	0.9893	0.0125	0.0000	0.9708	0.0000
14	-16.24	0.9670	0.0102	0.0476	0.0102	1.0508	1.0508	0.0494	0.0097	0.9780	-0.0143
15	-14.99	0.9630	0.0000	-0.3898	0.0003	0.2748	0.2748	-0.4048	0.0010	0.8719	-0.0015
16	160.73	0.9840	0.0000	-0.6830	0.0008	0.1960	0.1960	0.6941	0.0041	-0.8278	-0.0060
17	-19.41	0.9800	0.0000	0.3510	0.0002	1.5888	1.5888	0.3581	0.0001	1.0606	-0.0002
18	-22.89	0.9700	0.0000	0.0959	0.0000	1.1380	1.1380	0.0988	0.0000	0.9922	0.0000
19	-21.66	0.9850	0.0000	0.1365	0.0000	1.2205	1.2205	0.1386	0.0000	1.0162	0.0000
20	-3.43	1.0050	0.0828	-0.0214	0.0828	0.9790	0.9790	-0.0093	0.0846	0.9927	-0.1248
21	16.95	1.0250	0.4234	0.2431	0.4238	1.5919	1.5919	0.3950	0.2662	1.0093	-0.3927
22	-7.38	0.9550	0.0718	0.0055	0.0718	0.9733	0.9733	0.0156	0.0738	0.9503	-0.1089
23	-15.24	0.9520	0.0000	0.2006	0.0001	1.3102	1.3102	0.2107	0.0001	0.9994	-0.0001
24	-15.01	0.9540	0.0000	-0.1625	0.0000	0.6645	0.6645	-0.1703	0.0001	0.9157	-0.0001
25	15.23	0.9850	0.3754	0.1946	0.3757	1.4716	1.4716	0.3451	0.2553	0.9626	-0.3766
26	17.93	0.9950	0.2325	-0.0610	0.2326	0.9758	0.9758	0.0392	0.2384	0.9180	-0.3516
27	-6.72	0.9980	0.0000	0.0518	0.0000	1.0862	1.0862	0.0519	0.0000	1.0097	0.0000
28	46.77	1.0050	0.8522	0.1394	0.8534	1.9028	1.9028	0.7329	0.4485	0.8217	-0.6616
29	49.45	1.0500	0.8544	0.0152	0.8555	1.7525	1.7525	0.6512	0.4882	0.7920	-0.7200
30	54.74	1.0350	0.7470	-0.1027	0.7479	1.5028	1.5028	0.5320	0.4977	0.7180	-0.7340
31	-7.44	0.9840	0.0000	0.3031	0.0002	1.5076	1.5076	0.3080	0.0001	1.0533	-0.0002
32	-8.97	0.9800	0.0000	-0.1114	0.0000	0.7867	0.7867	-0.1137	0.0000	0.9544	0.0000
33	-8.06	0.9910	0.0000	0.0966	0.0000	1.1567	1.1567	0.0975	0.0000	1.0129	0.0000
34	171.28	0.9580	0.0000	-0.6378	0.0007	0.1739	0.1739	0.6658	0.0042	-0.8082	-0.0062
35	-8.25	0.9430	0.0000	0.2244	0.0001	1.3475	1.3475	0.2379	0.0001	0.9965	-0.0001
36	-3.32	1.0060	0.0000	0.1723	0.0000	1.2972	1.2972	0.1713	0.0000	1.0445	-0.0001
37	41.43	1.0400	0.7425	0.1727	0.7434	1.7956	1.7956	0.6049	0.4140	0.9034	-0.6107
38	2.53	0.9850	0.0000	-0.2469	0.0001	0.5588	0.5588	-0.2507	0.0002	0.9286	-0.0003
39	1.54	1.0150	0.0017	0.0048	0.0017	1.0231	1.0231	0.0047	0.0017	1.0161	-0.0025
40	66.04	1.0050	0.8820	-0.0083	0.8833	1.7919	1.7919	0.7262	0.4929	0.7208	-0.7271
41	3.26	0.9850	0.0000	0.1972	0.0001	1.3254	1.3254	0.2002	0.0001	1.0300	-0.0001
42	3.30	0.9800	0.0000	-0.1310	0.0000	0.7528	0.7528	-0.1336	0.0000	0.9499	-0.0001
43	-176.34	0.9900	0.0000	-0.9357	0.0015	0.6167	0.6167	0.9451	0.0024	-0.7773	-0.0035
44	-2.98	1.0100	0.0000	-0.1758	0.0001	0.7141	0.7141	-0.1740	0.0001	0.9708	-0.0001
45	36.88	1.0170	0.7087	0.2691	0.7096	1.8860	1.8860	0.6434	0.3762	0.9370	-0.5549

Table B.91
Initial condition of synchronous generator and condenser (part 2)

Node	AGG	VT	PG	QG	TQG	EF	CF	CDD	CQQ	FGD	FGQ
46	11.25	1.0100	0.4357	0.8225	0.4371	2.5045	2.5045	0.9049	0.1745	1.1698	-0.2575
47	-8.32	0.9710	0.0000	0.0992	0.0000	1.1446	1.1446	0.1021	0.0000	0.9940	0.0000
48	170.41	0.9650	0.0000	-0.8010	0.0011	0.4461	0.4461	0.8301	0.0026	-0.7782	-0.0038
49	-12.47	0.9520	0.0000	0.0325	0.0000	1.0100	1.0100	0.0341	0.0000	0.9597	0.0000
50	-11.91	0.9730	0.0000	0.0104	0.0000	0.9911	0.9911	0.0106	0.0000	0.9754	0.0000
51	-8.67	0.9800	0.0157	-0.0008	0.0157	0.9790	0.9790	-0.0004	0.0160	0.9796	-0.0236
52	-15.01	0.9750	0.0000	0.0415	0.0000	1.0473	1.0473	0.0426	0.0000	0.9846	0.0000
53	-16.26	0.9930	0.0000	0.0387	0.0000	1.0593	1.0593	0.0390	0.0000	1.0018	0.0000
54	-3.07	1.0050	0.0000	0.0376	0.0000	1.0686	1.0686	0.0374	0.0000	1.0134	0.0000